Pequeño manual introductorio de tecnologías para el *marketing* digital electoral

El caso de las candidaturas
a la Alcaldía de Bogotá 2019



K

Pequeño manual introductorio de tecnologías para el *marketing* digital electoral

El caso de las candidaturas a la Alcaldía de Bogotá 2019

Stéphane Labarthe
Víctor Práxedes Saavedra
Pilar Sáenz

Fundación Karisma



En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos. Más información sobre el tema en http://www.documentoaccesible.com/#que-es.

Esta publicación fue realizada por la Fundación Karisma con el apoyo y financiación de Indela.

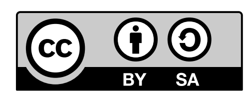


Autores
Stéphane Labarthe
Víctor Práxedes Saavedra
Pilar Sáenz

Revisión de estilo
Felipe Useche

Diseño editorial y gráfico
Cuántika Studio

Bogotá, Colombia
2020



Esta publicación está disponible bajo una Licencia Creative Commons Reconocimiento Compartirigual 4.0. Para ver una copia de esta licencia, visite https://creativecommons.org/licenses/by-sa/4.0/deed.en.

Este libro se complementa con una serie de anexos que dan mayor detalle de las pruebas realizadas y sus resultados. A lo largo del texto, se irá haciendo referencia a estos y pueden consultarse en el sitio web de Fundación Karisma: https://tediel.karisma.org.co

Contenido

Introducción

Internet ha cambiado nuestras vidas. La frase suena tonta, obvia. Pero es justamente una reacción así, a la que hoy en día es una realidad evidente, lo que causa curiosidad. A medida que avanzan los años e internet cumple 10, 20 y ya casi 30 años, nos vamos percatando de las formas en que su existencia ha afectado profundamente nuestras vidas. Nuestra interacción social ocurre alrededor de las redes sociales, los temas de conversación, las relaciones de amistad y pareja, cómo leemos, escribimos, cómo investigamos y hasta cómo nos divertimos. Internet ha cambiado las reglas del juego de miles de negocios, desde el cine a los bancos, pasando por la prensa, la industria musical que han significado cambios de paradigma y crisis para aquellas empresas que no han sabido seguir el paso de la transformación digital. Algunos celebran esta renovación, a veces forzada y siempre forzosa, de la experiencia humana, y otros la rechazan, con buenas o malas razones, pero un campo particularmente contencioso del debate es el papel de internet y las tecnologías digitales en la política.

Para muchos, una cosa es que las cadenas televisivas hoy transformen sus propuesta de contenido porque su audiencia no logra alcanzar los números de un muchacho sueco que se graba desde su casa mientras juega en el pc. Otra, que ese mismo mundo del internet se introduzca en la esfera política y que, para algunos, esto llegue a implicar un debilitamiento de las instituciones de la democracia. Cada tanto aparece alguna noticia que nos invita a reevaluar el poder de internet: hace unos años hablábamos de Assange o Snowden, hoy, de Cambridge Analytica y Nation Builder, y aunque todos son casos muy distintos, cada uno de ellos es una expresión de cómo internet está cambiando nuestras vidas y, en los últimos dos casos, de cómo, quizás, las dinámicas propias de internet pueden haber transformado el modo en que se hace política desde ahora, con consecuencias que todavía no se comprenden del todo y, con razón, nos preocupan como ciudadanos.

Este, entonces, es un manual de supervivencia para los tiempos convulsos en los que internet y la política chocan entre sí. Una guía para la ciudadanía en la era de las tecnologías de la información y comunicación que, hábil en navegar el mar de mentiras e imprecisiones de la política tradicional, ahora necesita más herramientas para leer a través de las capas de tecnología en las que hoy se explayan las campañas electorales. Esta también es una guía para las personas que aspiran a incursionar en la política, que ven esta intrusión de internet en el mundo electoral como una oportunidad de participación democrática, pero necesitan familiarizarse con ese mundo, sus reglas, y sobre todo, sus límites prácticos y legales.

Este manual entonces tiene dos objetivos:

- Aportar a la ciudadanía de rudimentos básicos sobre internet y su uso en campañas, así como unas herramientas mínimas que puedan aplicar en el futuro para obtener más información respecto a cómo se relaciona una campaña con el electorado a través de la Red.

- Contribuir a incrementar las capacidades de las directivas de campaña por medio de un conocimiento mínimo y necesario para interactuar de modo responsable con el electorado a través de internet.

¿Por dónde empezar? Por la infraestructura, sin ella, internet es pura metáfora. Por eso esta guía es un curso acelerado también de cómo funciona internet, dónde está, cómo nos relacionamos con páginas web, cómo nos rastrean y cómo otros pueden seguir lo que hacemos en internet, para impactarnos con publicidad dirigida.

¿Cómo lo vamos a hacer? A través del estudio de las campañas electorales para la Alcaldía de Bogotá de 2019. Iremos intercalando las partes teóricas con su aplicación práctica en relación a las cuatro candidaturas principales. Parte de esa teoría presenta algunas de las pruebas técnicas que realizamos desde Fundación Karisma, con el objetivo de que quienes lean puedan, en futuras ocasiones, replicarlas. De igual manera, para poder tener una visión global de cómo nos relacionamos digitalmente con las campañas, mostraremos cómo lo han hecho unas “ciudadanas virtuales” que creamos para ello. Finalmente, dado que la temática tiene implicaciones importantes en términos de protección de datos, daremos unas pinceladas sobre el ordenamiento jurídico aplicable en relación con los casos de estudios mencionados.

¿Qué podemos aprender de las campañas con lo que aquí descubrimos? Tras la lectura del manual, podremos saber dónde están físicamente los sitios web de las campañas, qué herramientas de rastreo web son comunes y si cumplen con las obligaciones jurídicas que establece el ordenamiento colombiano. Como verán, ni siempre se cumplen las obligaciones jurídicas ni las herramientas tecnológicas que se usan se utilizan correcta o racionalmente. Sin embargo, antes de buscar la mala fe, que puede que la haya, no olvidemos el principio de la Navaja de Hanlon: “nunca atribuyas a la maldad lo que puede ser explicado por la estupidez”. ¡Buen viaje!

Un mapa para internet



Primero lo primero. Por más sofisticadas que sean las técnicas de rastreo o "inteligentes" las estrategias de publicidad dirigida, todas tienen que respetar las reglas de la infraestructura tecnológica en la que se cimentan. Entender esos rudimentos no sólo hace las veces de glosario para el resto del texto, sino que nos da una idea del mundo en el que se mueven las campañas electorales digitales, algo así como ver el mapa de una ciudad que se quiere visitar antes de ir, para hacerse una idea general de cómo uno podría moverse en ese espacio.

Esta sección, por supuesto, no sustituye estudios en ciencias de la computación (que incluye, por poner ejemplos, grados como la ingeniería de sistemas, en Colombia, o la ingeniería en informática, en Argentina), pero sí provee de unos rudimentos básicos que permitan comprender a quien lee la totalidad del informe sin necesidad de recurrir a fuentes externas. De igual manera, muchos de los términos acá explicados se usan con cierta regularidad sin hacer precisión sobre qué son, como dirección IP o *cookie*, de modo que la guía comienza por aclarar varios de ellos. Por este motivo, si usted tiene un conocimiento avanzado en la materia, detectará fácilmente omisiones y simplificaciones que, sin embargo, esperamos no impidan lograr el objetivo de compartir el conocimiento técnico necesario para entender todo el informe. Las personas con un conocimiento versado son libres de saltarse este capítulo, para las demás, continuemos…

Estructura básica de internet

El entorno en el que se desarrollan las pruebas comentadas en este informe es internet, una red (de redes) a través de la cual nos conectamos en distancia para compartir información. Podemos decir que la red se compone de forma simplificada de tres partes:

- Infraestructura: La parte material de internet, hablamos de los computadores, teléfonos, cables de distintos tipos, antenas, los *router* que nos instalaron en la casa y demás.

- Protocolos: Las reglas que permiten que los dispositivos (como teléfonos y computadores) se comuniquen a través de la red.

- Contenidos: La razón de ser de internet, los textos, imágenes, videos, audios, páginas web, correos y el largo etc de recursos, que transitan por la infraestructura de acuerdo con unas reglas establecidas o protocolos, y que son la razón por la que nos conectamos.

Muchas de las comunicaciones que hacemos en la red lo que pretenden es acceder a contenidos de una página web que están alojados en un computador distinto al nuestro. Este tipo de comunicación se denomina **cliente-servidor**. El equipo que solicita la información, se denomina **cliente** y éste le pide a otro computador, llamado **servidor**, el acceso a ella.

Esta comunicación cliente-servidor requiere unos protocolos sin los cuales no sería posible internet, dado que de éstos depende que la información se transmita entre máquinas, las cuales deben seguir reglas estrictas. El primer protocolo que nos interesa es el **IP** (*Internet Protocol* - Protocolo de Internet) a través del cual obtenemos la famosa dirección IP: una serie números, similar a una dirección postal, que identifica las máquinas para establecer comunicación entre ellas. Sin embargo, cuando intentamos acceder a una página web, no solemos usar una serie de números, así como cuando llamamos a alguien no usamos su cédula, sino su nombre. Las páginas web tienen de manera similar un nombre de dominio. Más adelante, al hablar de las pruebas de resolución de dominio y *whois*, entraremos en más detalle pero en este punto sabemos que cuando introducimos el nombre de dominio en nuestro navegador, nuestro equipo consultará cuál es la dirección IP que corresponde a ese nombre en una máquina que tiene una especie de páginas amarillas de internet, para poder “llamar” al servidor donde está alojada la página. Estas máquinas son los servidores de referencia DNS, de los que tratamos en la siguiente sección.

La importancia de conocer la dirección radica en que la página web se encuentra físicamente en otro computador al que hay que consultar. Estos computadores que responden a diferentes tipos de consultas son, como ya señalamos, los servidores. Los hay de varios tipos, este en particular que aloja —hospeda— las páginas es llamado *host*, de donde proviene la palabra ***hosting***, que es el servicio de proveer los espacios donde las páginas web se alojan. Este servicio lo proveen compañías dedicadas. Si no existiesen y quisiéramos crear una web y ponerla a disposición de todo el mundo, tendríamos que tener un computador (donde estaría alojada la página) todo el día conectado y, aún así, puede que no tuviera la capacidad de entregar la información si muchas personas intentan consultarla a la vez.

El último concepto que necesitamos para entender lo que hay detrás de lo que llamamos dirección web es URL (*Uniform Resource Locator* - Localizador Uniforme de Recursos). Cuando uno dice *¿cómo es la dirección web?* o *¿en qué página está?* la URL es lo que a uno se suele referir. Es la ruta completa a un recurso, como ese vídeo de gatos. En la siguiente tabla se resumen lo aprendido:

Imaginemos la siguiente dirección web en la que están los vídeos de gatos: http://www.videoscheveres.co/videosdeanimales/gatos.html		
URL	gatos.html	recurso o archivo
	videosdeanimales/	subdirectorio en el dominio
	videoscheveres.co/	nombre del dominio
Protocolo	http	protocolo de comunicación. Lo veremos más adelante
IP	24.256.37.4.0	lo que nos dará el servidor de dominio si le preguntamos por el nombre de dominio

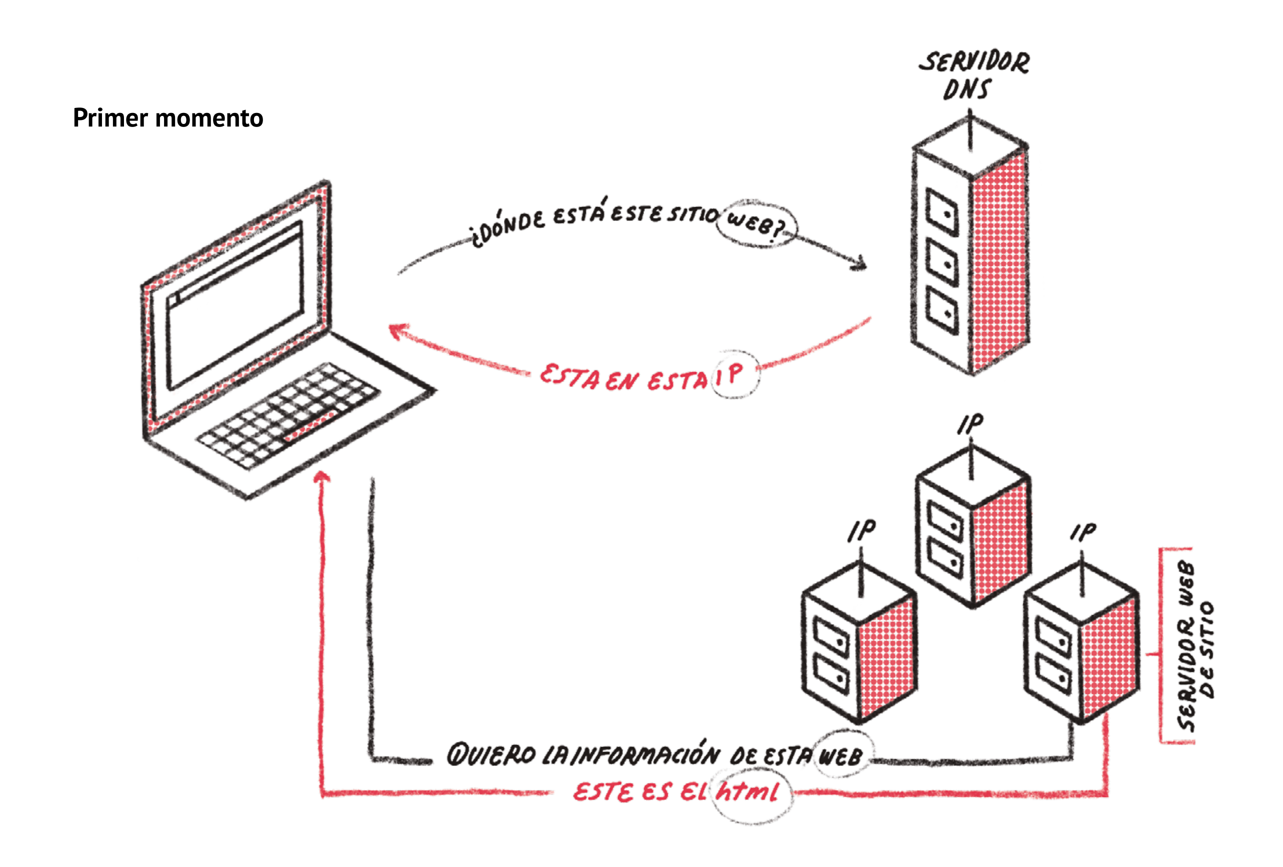
Herramientas para conocer dónde está una web

Como vimos arriba, para comunicarse con un servidor web, nuestro dispositivo usa el protocolo IP al establecer una comunicación con otra máquina, en nuestro caso el servidor web. Para obtener la dirección IP a partir del nombre de dominio, nuestro dispositivo hace lo que se conoce como una "**resolución de dominio**" hacia servidores de referencia. Tanto el protocolo usado para hacer esta resolución cómo estos servidores de referencia se llaman "DNS" (*Domain Name System* - Sistema de Nombres de Dominio). Si los servidores web eran computadores cuya función es enviarnos una página cuando la solicitamos como cliente, los servidores de referencia tienen como función decirle a nuestra máquina cuál es la dirección IP vinculada con el nombre de dominio que introdujimos en el navegador. Como lo mencionamos antes, los servidores de referencia pueden entenderse como unas páginas amarillas o una vieja guía telefónica. Nuestro computador consulta automáticamente al solicitar una web o podemos hacerlo de forma manual con comandos como `host`, `nslookup`.

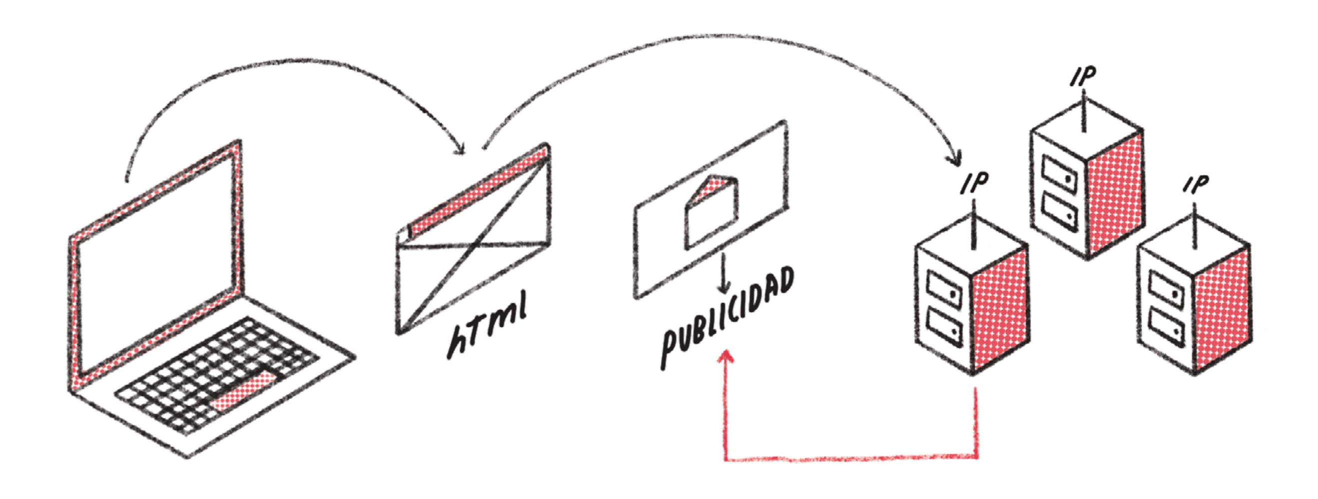
¿Y para qué querríamos conocer la dirección IP? Porque a través de ella podemos obtener otra información como la empresa que hace el *hosting* de la web, la fecha en que se registró, cuándo caduca, entre otras. En nuestros análisis, esto nos permitió saber dónde físicamente se encontraban las páginas de las candidaturas[1]. Para ello, se utiliza el cuarto protocolo que presentaremos en este texto: el protocolo ***whois*** (literalmente "quién es"). Este es simplemente un conjunto de reglas para preguntas y respuestas dirigidas a interrogar a las bases de datos de dominios y direcciones IP y obtener más información. Para ello, el comando que utilizamos es `whois`.

1. Hemos hablado hasta aquí de páginas web, pero ha de aclararse que estas son un único "documento". Cuando introducimos el nombre de dominio, nos enviará a una página, pero esta mostrará enlaces a otras páginas web, alojadas en el mismo servidor web. Por ejemplo, en la página principal de Claudia López encontramos enlaces a "propuestas", "mi historia", entre otras. Cada uno de esos enlaces lleva a otra página web. El conjunto de estas páginas web, con el dominio común, se denomina sitio web. Muchas veces veremos que ambos conceptos, página y sitio, se utilizan indistintamente y no afecta a la comunicación, pero no son exactamente lo mismo.

Primer momento



Segundo momento



La siguiente captura muestra un ejemplo del uso de ambas herramientas. Cada línea verde supone un uso de comandos desde nuestra computadora. En la primera, vemos el uso del comando `host` y la información que arroja (la dirección IP de la *web* y del servicio de correo vinculador). En la segunda, vemos el uso del comando `whois` y parte de la información que devuelve.

```
k-lab@klab-Inspiron-7559:~$ host claudia-lopez.com
www.claudia-lopez.com is an alias for claudia-lopez.com.
claudia-lopez.com has address 23.227.38.32
claudia-lopez.com mail is handled by 10 78.142.63.52.
k-lab@klab-Inspiron-7559:~$ whois 23.227.38.32

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.
#


NetRange:       23.227.32.0 - 23.227.63.255
CIDR:           23.227.32.0/19
NetName:        SHOPIFY-NET
NetHandle:      NET-23-227-32-0-1
Parent:         NET23 (NET-23-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS62679
Organization:   Shopify, Inc. (SHOPI-1)
RegDate:        2013-09-19
Updated:        2013-09-19
Ref:            https://rdap.arin.net/registry/ip/23.227.32.0


OrgName:        Shopify, Inc.
OrgId:          SHOPI-1
Address:        150 Elgin Street, 8th Floor
City:           Ottawa
StateProv:      ON
PostalCode:     K2P 1L4
```

Hasta aquí...

- Hemos aprendido la estructura de internet en cuanto a las relaciones cliente-servidor para consultar páginas web.
- Hemos conocido el protocolo IP como conjunto de reglas que rigen esas relaciones.
- Hemos introducido los comandos `host`, `nslookup` y `whois` para conocer cómo se da esa relación en un caso concreto.

Ejercicios concretos: el caso de las elecciones para bogotá 2019

Hasta ahora, hemos presentado conceptos fundamentales para entender cómo funciona internet. Sin embargo, es hora de ponerlos en práctica. Para ilustrar las ideas que presentamos en esta guía, hemos decidido estudiar las campañas electorales de los cuatro principales candidatos a la alcaldía de Bogotá de 2019, enfocándonos, sobre todo, en la privacidad y la presencia de herramientas de rastreo y de *marketing* político. Usando lo aprendido en la primera sección, estos son los datos principales de nuestro caso de estudio.

Los sitios web analizados son los siguientes:

- El sitio web de Claudia López: www.claudia-lopez.com
- El sitio de Carlos Fernando Galán: www.bogotaparalagente.com
- El sitio de Hollman Morris: www.hollmanmorris.co
- El sitio de Miguel Uribe Turbay: www.migueluribeturbay.co

Con las herramientas descritas anteriormente, y para determinar en dónde acaban los datos de los usuarios de estas páginas, analizamos la dirección IP de los servidores web de los sitios de los cuatro candidatos y buscamos a quién pertenecían y dónde se localizaban (ver anexo "¿Dónde están mis datos?"), resumiendo los resultados en la siguiente tabla.

Servidor web	Dirección IP	País / Estado	Empresa de hosting
www.claudia-lopez.com www.esconelverde.com	23.227.38.32 (hosting principal) 23.235.211.194 (datos personales)	Canadá (hosting principal) Estados Unidos, California (CA) (datos personales)	Shopify Inc. (hosting principal) In Motion Hosting Inc. (datos personales
www.bogotaparalagente.com	13.59.55.62	Estados Unidos, Washington (WA	Amazon Technologies Inc.
www.hollmanmorris.co	160.153.132.207	Estados Unidos, Arizona (AZ)	GoDaddy.com
www.migueluribeturbay.co marketing.migueluribeturbay.com	18.233.228.16 (hosting principal) 174.129.173.245 (subdominio de *marketing*)	Estados Unidos, Washington(WA)	Amazon Technologies Inc. Amazon Web Services Inc.

Como segundo paso, analizamos los flujos de datos[2] en los formularios para determinar su destino, ya que a veces los datos pueden ser remitidos a un servidor distinto al que aloja la página web. Efectivamente, encontramos que en el sitio web de Claudia López, los datos personales se enviaban a otro servidor con dominio "esconelverde.com" (ver anexo "Envío de datos personales a otros servidores"). Es por ello que se relaciona de modo separado en la tabla anterior.

2. En el siguiente capítulo nos meteremos en la cuestión de cómo fluyen los datos por la Red. La mención aquí es, sin embargo, necesaria para observar que algunos candidatos utilizan servidores distintos, en distintos lugares, para según que servicios. Lo mismo se aplica al caso de Miguel Uribe Turbay y las *cookies*.

En cuanto al servidor de la página principal de la candidata Claudia López, el hecho de que sea alojado por la empresa Shopify Inc. es interesante: **esta empresa provee soluciones integradas de *e-commerce*** (sitio web, *marketing* por *e-mail* y redes sociales) para “construir un negocio” (ver anexo “Capturas de pantalla del sitio web de Shopify”).

En el caso de Miguel Uribe Turbay, la existencia de un subdominio de *marketing* —que aparece más adelante en la sección sobre *cookies*— ya permite apreciar el componente de publicidad en línea del sitio web. Además, el hecho de que sea alojado en un servidor de una dirección IP distinta al de la web principal, apunta a que el servicio asociado está situado en un servidor de la empresa correspondiente (en este caso, Mautic) que, si bien también está alojado en Amazon, no es el mismo servidor de hosting de la web principal.

La ubicación de los servidores de almacenamiento de estos datos personales puede tener impacto en relación a la normativa de protección de datos aplicable. Es por ello que ciertas legislaciones, como la colombiana, prohíben las transferencias de datos personales hacia países que no tienen un nivel adecuado de protección, con algunas excepciones como la existencia de una *información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia* (artículo 26, Ley 1581). Los países considerados en Colombia como con un nivel de protección de datos adecuado se encuentran listados en la Circular Externa 005 de la Superintendencia de Industria y Comercio, del 10 de agosto del 2017[3]. En cuanto a los países que nos interesan aquí: Canadá no figura en la lista; Estados Unidos, sí. Sin embargo, la inclusión en esta lista de Estados Unidos —que no cuenta con una ley de protección de datos (con excepción de California)— ha sido y sigue siendo objeto de crítica[4].

3. Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf

4. Ver por ejemplo este artículo, escrito por Nelson Remolina, actual Superintendente Delegado de Protección de Datos: https://habeasdatacolombia.uniandes.edu.co/?p=2536

Caminando por el mapa de internet



En la gran mayoría de los casos las páginas web están escritas en un lenguaje de programación llamado HTML (*HyperText Markup Language*) que es interpretado y ejecutado por nuestro navegador. Un lenguaje de programación no es más es un lenguaje, como el español o el inglés, con reglas gramaticales definidas que permite a una persona escribir —programar— una serie de instrucciones para controlar una computadora. Hablamos de código fuente como el conjunto de líneas de texto escritas en ese lenguaje que es interpretado por nuestro navegador y enviado al servidor en forma de instrucciones para poder visualizar la página como usuarios.

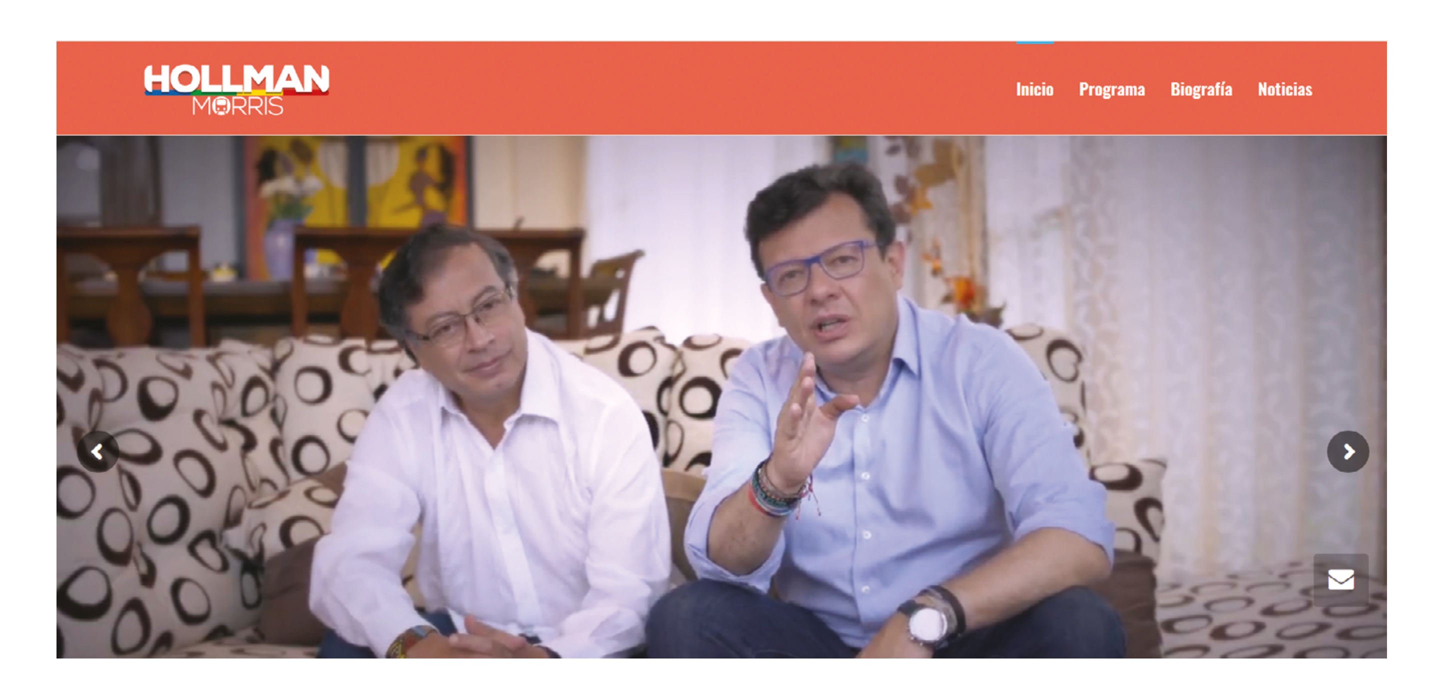
Ahora bien, muchas veces las páginas que vemos contienen objetos que son externos al código fuente. Por ejemplo, cuando aparece un vídeo de YouTube en nuestra página de noticias favorita, el vídeo no ha sido enviado directamente desde el servidor de la web de noticias, sino ha sido "referenciado" por el código fuente para que nuestro computador vaya a otro servidor, el de YouTube en este caso, para obtener el vídeo. Estos **recursos externos** pueden ser también sonidos, imágenes, videos y funciones programadas en otro lenguaje llamado Javascript. Cuando en una página web están presentes servicios de terceros, llegaron aquí porque quien administra la página les "abrió la puerta". Esto se hace generalmente mediante la inclusión en el código fuente (HTML) de la página web de porciones de códigos externos entregados por estos terceros, sean YouTube, Soundcloud, Instagram, Flickr o la página que sea.

En un muchos casos se trata de una referencia a una imagen externa o de una función en lenguaje Javascript directamente incluida en el código fuente o alojada en un servidor web externo. Hablamos entonces de "***tags***" de terceros, fragmentos de código que nos permiten realizar la medición y seguimiento de las visitas, por ejemplo o de porciones completas de código en Javascript, "***scripts***" que permiten incluir acciones interactivas como formularios, presentaciones o validaciones de información, entre muchas otras cosas. *Tags* y *scripts* nos interesan porque se utilizan mucho en el contexto

del *marketing* digital[1]. Esto es así dado que la ejecución de estos suele iniciar una comunicación con el servidor web de la empresa de *marketing* digital, distinto del de la página web que visitamos, junto con transmisiones de datos personales a esta empresa a través de, por ejemplo, las *cookies* a las que nos referiremos más adelante.

Lo que hemos visto en relación a páginas web es también aplicable a los **correos electrónicos** que leemos puesto que se construyen también utilizando el lenguaje HTML.

¿Cómo vemos la web?



1. Los anexos "Uso de la herramienta ROI Hunter Easy en el sitio de Claudia López", "Instalación de la *cookie* de Doubleclick en el sitio de la campaña de Miguel Uribe Turbay", "Herramientas *marketing* y rastreo en el sitio de la campaña de Miguel Uribe Turbay", "Uso de técnicas de *fingerprinting* en el sitio de la campaña de Miguel Uribe Turbay" muestran ejemplos concretos de *tags* y *scripts* en el contexto del *marketing* digital.

¿Cómo está escrita?

```
<!DOCTYPE html>
<!--[if lt IE 7]>
<html class="no-js lt-ie9 lt-ie8 lt-ie7" lang="es-CO"><![endif]-->
<!--[if IE 7]>
<html class="no-js lt-ie9 lt-ie8" lang="es-CO"><![endif]-->
<!--[if IE 8]>
<html class="no-js lt-ie9" lang="es-CO"><![endif]-->
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="es-CO"><![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="es-CO">
<!--<![endif]-->
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=9; IE=8; IE=7; IE=EDGE"/>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="profile" href="http://gmpg.org/xfn/11">
    <link rel="pingback" href="https://hollmanmorris.co/xmlrpc.php">

    <!-- Fav and touch icons -->
            <link rel="shortcut icon" href="https://hollmanmorris.co/wp-content/uploads/2018/10/ico.png">
                <link rel="apple-touch-icon-precomposed" href="https://hollmanmorris.co/wp-content/uploads/2018/10/ico.png">
                <link rel="apple-touch-icon-precomposed" sizes="72x72" href="https://hollmanmorris.co/wp-content/uploads/2018/10/ico.png">
                <link rel="apple-touch-icon-precomposed" sizes="114x114" href="https://hollmanmorris.co/wp-content/uploads/2018/10/ico.png">
                <link rel="apple-touch-icon-precomposed" sizes="144x144" href="https://hollmanmorris.co/wp-content/uploads/2018/10/ico.png">

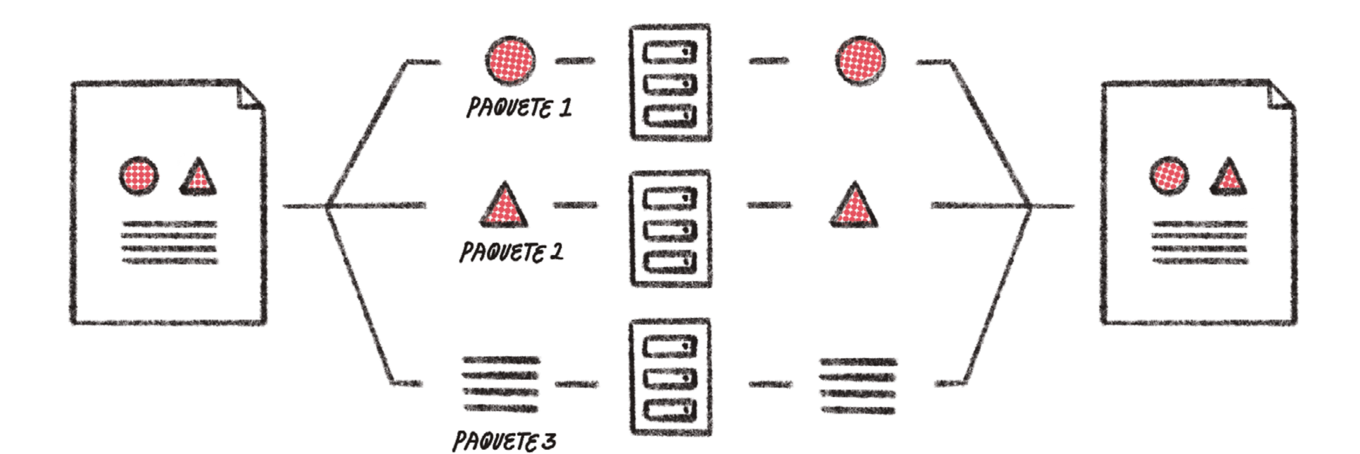
    <!-- HTML5 shim, for IE6-8 support of HTML5 elements -->
    <!--[if lt IE 9]>
    <script src="https://hollmanmorris.co/wp-content/themes/kleo/assets/js/html5shiv.js"></script>
    <![endif]-->

    <!--[if IE 7]>
    <link rel="stylesheet" href="https://hollmanmorris.co/wp-content/themes/kleo/assets/css/fontello-ie7.css">
    <![endif]-->


    <title>Hollman Morris &#8211; Hollman Morris</title>
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
```

Paquetes de datos (http)

Una vez conocemos cómo se nombran dos puntos a través del protocolo IP, es necesario saber cómo se transmite la información entre ellos. Esto se hace a través de paquetes de datos (de los que hablaremos y pondremos ejemplos más abajo) que cuentan con una capacidad limitada de enviar toda la información que estamos solicitando. Aquí es donde entra en juego el **protocolo TCP** (*Transmission Control Protocol* - Protocolo de Control de Transmisión). Este se encarga de dividir la información en paquetes para que sea posible transmitirla a través de la red con cierta velocidad y, además, se encarga de volver a ensamblar los paquetes cuando son recibidos por el computador o dispositivo de destino. Utilizando un símil, si estuviéramos enviando por correo tradicional un texto de varias páginas, el TCP sería el conjunto de reglas tanto para dividir el texto en varios sobres para ser enviado de forma manejable, como, en destino, las reglas para recomponer el documento y entregarlo al usuario final como si nunca hubiera sido dividido.



Cómo ya lo hemos explicado, la estructura de internet se compone de distintas capas, desde la infraestructura que procesa la información (computadores) y las transmite de diferentes formas: luz (fibra óptica), electricidad (cable ethernet) u ondas electromagnéticas (4G, WIFI, Bluetooth, etc.) hasta la capa más alta que es la capa de contenidos. De forma análoga, los protocolos se encajan unos dentros de otros como *matrioshkas*, "muñecas rusas", cada uno muestra la información correspondiente a su "capa" y contiene la siguiente.

Hemos visto ya, dos de estos protocolos el IP y el TCP. Ahora agregaremos otro: el HTTP. **HTTP** (*Hypertext Transfer Protocol* - Protocolo de Transferencia de Hipertexto) es otro de los conjuntos de reglas que permiten nuestra comunicación por internet. Si la función del protocolo IP era saber dónde encontrar a los actores de la comunicación y la función del protocolo TCP es regir cómo se divide y unifica la información, la función del protocolo HTTP es establecer las reglas de comunicación entre cliente y servidor de modo que estos dos equipos "hablen" la misma lengua. Esto es necesario porque, cuando solicitamos una página *web a un servidor*, estamos "preguntando" y la información que recibimos es la "respuesta", pero tanto cliente como servidor deben hablar en los mismos términos, o de lo contrario no podríamos ver nada, simplemente porque cliente y servidor no se "entienden". En esa lógica, el protocolo HTTP es el responsable de que la relación cliente-servidor se convierta en una relación de comunicación, de pregunta-respuesta. Establece la forma (sintaxis) y significados (semántica) al igual que nuestro español requiere que el que habla y el que escucha compartan un vocabulario en común y una serie de reglas de cómo organizar las frases, conjugar verbos o incluso pronunciar los sonidos de las palabras, por ejemplo. En este caso, la sintaxis y la semántica comparten su significado del mundo real en el virtual.

Aunque nos vamos a centrar en la forma y contenido de los paquetes HTTP más adelante, cuando hablemos de herramientas de rastreo, ya encontramos un primer impacto en este sentido porque cuando un servidor web recibe un paquete HTTP(S), debe recibir los paquetes IP. El servidor recibe la muñeca rusa. Esto significa que también recibe la dirección IP del dispositivo que también pueden servir para rastrear el usuario por ser los identificadores de su equipo.

HTTP y HTTPS

A lo largo del texto, nos referimos a HTTP como protocolo de comunicación y transferencia de información. Sin embargo, vemos que muchas veces nos encontramos con una sigla similar: HTTPS. **HTTPS** (en inglés, *Hypertext Transfer Protocol Secure*) es la combinación del protocolo de comunicación HTTP con otros protocolos de cifrado que permiten que dicha comunicación sea segura. Estos protocolos se llaman SSL (*Secure Sockets Layer* - Capa de Puertos Seguros) y TLS (*Transport Layer Security* - Seguridad de la Capa de Transporte). Estos protocolos cifran la comunicación entre el cliente y el servidor, de modo que nadie más que ellos dos pueden conocer el contenido de la misma. Es decir, cualquier persona que capture el flujo de la comunicación (como nuestro proveedor de internet, las autoridades, etc) pueden saber que nos estamos comunicando con un servidor pero no cuál es el contenido de esa comunicación.

El paquete HTTPS no es, sin embargo, esencialmente distinto al HTTP, sino que puede entenderse como un paquete HTTP encapsulado en un protocolo de seguridad, bien sea SSL o TLS. Por eso, durante el texto usaremos la expresión "paquete HTTP(S)" para designar ambos sin distinción, salvo que ésta sea relevante para el caso particular.

Hasta aquí...

- Hemos profundizado en cómo funciona la comunicación en internet a través del lenguaje **HTML**, los **protocolos TCP** y **HTTP(S)**.
- Nos hemos acercado, pero no mucho, a la idea de seguridad digital al conocer cómo el protocolo de comunicación HTTP se puede combinar con protocolos de cifrado como SSL y TLS para, bajo las siglas HTTPS, poder tener una comunicación segura.

Los protocolos que hemos estudiado hasta ahora se pueden observar cuando vemos un paquete de datos que se transmite en una comunicación entre el cliente y el servidor. Cada transmisión de información se denomina una "trama de red" (*frame*). Esta unidad de envío de datos contiene información respecto de todos los protocolos vistos hasta ahora. Veamos con un ejemplo práctico cómo se presentan. El gráfico siguiente es una trama de red, obtenida con una herramienta de captura de tráfico como Wireshark[2], de una solicitud hacia el servidor web de la página de Miguel Uribe Turbay.

```
› Frame 68: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on interface 0
› Ethernet II, Src: IntelCor_ce:6a:21 (84:ef:18:ce:6a:21), Dst: Technico_0e:66:f3 (58:23:8c:0e:66:f3)
› Internet Protocol Version 4, Src: klab-Inspiron-7559.local (192.168.0.43), Dst: migueluribeturbay.co (18.233.228.166)
› Transmission Control Protocol, Src Port: 43218 (43218), Dst Port: http (80), Seq: 1, Ack: 1, Len: 324
› Hypertext Transfer Protocol
```

Se observan las siguientes líneas con distinta información:

- Línea 1: Identificador de la trama de red. En este caso, *frame* 68 que contiene 390 *bytes*, habiendo sido todos capturados por la herramienta.
- Línea 2: Información relativa al protocolo Ethernet.
- Línea 3: Información relativa al protocolo IP. En este caso, nuestro equipo que es el Origen (`Src` por Source en inglés) con su nombre y

2. Este tipo de herramientas permiten hacer análisis de tráfico, esto es, observar qué circula por la red en la que estamos. Además de para los análisis que nos ocupan, pueden servir para detectar intrusiones o problemas de red y comenzar a solventarlos, obtener estadísticas sobre los flujos de red, entre otras.

dirección ip y el dominio e ip de la web de Miguel Uribe Turbay que es el Destino (`Dst` por Destination en inglés).

- Línea 4: Información relativa al protocolo TCP. Encontramos aquí, entre otra información, que el puerto de destino ("Dst port") es el puerto 80, el que por defecto permite a los servidores *web* escuchar nuestras preguntas.
- Línea 5 (En azul): Información sobre el protocolo HTTP.

Recapitulando: Ethernet, IP, TCP y HTTP a través de una llamada telefónica

Ya hemos visto gran parte de los protocolos que regulan la comunicación en internet, sin meternos en la profundidad de lo relativo a la infraestructura. Podemos entender estos protocolos si, salvando ciertas distancias, pensamos en un símil como una llamada telefónica:

- El teléfono en sí mismo, incluidas sus partes físicas como el micrófono, actúa como puerta a la infraestructura. Recoge y nos devuelve sonidos que lleva y trae a través de la red de telefonía. Las reglas que rigen cómo el micrófono traduce la voz a una señal eléctrica que se transmite a la red de telefonía y cómo lo que se recibe se emite por el auricular sería similar al protocolo **Ethernet**.
- Por su parte, nuestros números telefónicos son lo que marcamos para comunicarnos y nos permiten identificar el interlocutor con el que deseamos hablar. En ese sentido, nuestro número es como nuestra **dirección IP**.
- Pero no todo el mensaje lo emitimos a la vez, las oraciones se dividen en palabras y las palabras en sonidos. Las reglas que permiten la división en sonidos y la unión ordenada de los mismos para percibir palabras funcionan de modo análogo al protocolo **TCP**.
- Finalmente, el protocolo **HTTP** sería, en este caso, el equivalente al lenguaje en que nos comunicamos: español. Supone todas las reglas lingüísticas que permite que una sucesión de palabras se conviertan en un mensaje comprensible y transmisible.
- Y hablaríamos de **HTTPS** si los que estamos a ambos lados del teléfono, pero nadie más, conociésemos y usásemos una clave que hemos concertado previamente para que solo nosotros entendiésemos el mensaje. Por ejemplo, cambiando cada consonante y vocal por la siguiente en el abecedario, no nos saludaríamos con un "¡Hola!" sino con un "¡Jume!".

¿Y los paquetes en la elección a alcaldía?

Analicemos ahora un paquete HTTP(S)[3] a través de un ejemplo:

Este es el formulario que vamos a rellenar, corresponde al formulario de inscripción de la web de Miguel Uribe Turbay:



Y este es el contenido del paquete HTTP que se genera cuando rellenamos el formulario y damos *clic* a "inscribirme". Originalmente no tiene los colores mostrados, que se han añadido para poder distinguir las partes.

3. En caso de que quiera "bucear" más en cómo se comunican nuestros dispositivos por internet, el protocolo HTTP es definido en los documentos RFC 7230 (https://tools.ietf.org/html/rfc7230) y 7237 (https://tools.ietf.org/html/rfc7237).

```
POST /?cn-reloaded=1 HTTP/1.1
Host: www.migueluribeturbay.co
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.migueluribeturbay.co/?cn-reloaded=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 107
Cookie: PHPSESSID=07ofba8t8s6sdp23o7np8tplsq;
nvg56903=9da5f54b64b0b63c54f9ee57f09|2_266; _ga=GA1.2.1048251503.1569213115; _
gid=GA1.2.2074022322.1569213115; __utma=21743527.1048251503.1569213115.1569
213121.1569213121.1; __utmb=21743527.3.9.1569213347867; __utmc=21743527; __
utmz=21743527.1569213121.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
cookie_notice_accepted=true
Connection: keep-alive
Upgrade-Insecure-Requests: 1
name=Karolina+Uribe&email=karolinauribebogota%40gmail.
com&mobile_number=3173386007&contact_data=INSCRIBIRME
```

Observa que, en la parte roja, se encuentra exactamente la información que hemos introducido con los campos que requería el formulario. Así los podemos relacionar:

Nombre - `name=`

Email - `email=`

Celular - `mobile_number`

Un paquete HTTP(S) tiene tres componentes, cada una resaltada con un color diferente

- La verde es una línea de comando que incluye el método usado para enviar información al servidor, `POST` en este caso aunque también se suele utilizar otro método llamado GET[4], la subdirección en la URL donde está alojado el recurso (`/?cn-reloaded=1`) y la versión del protocolo, (`HTTP/1.1`),

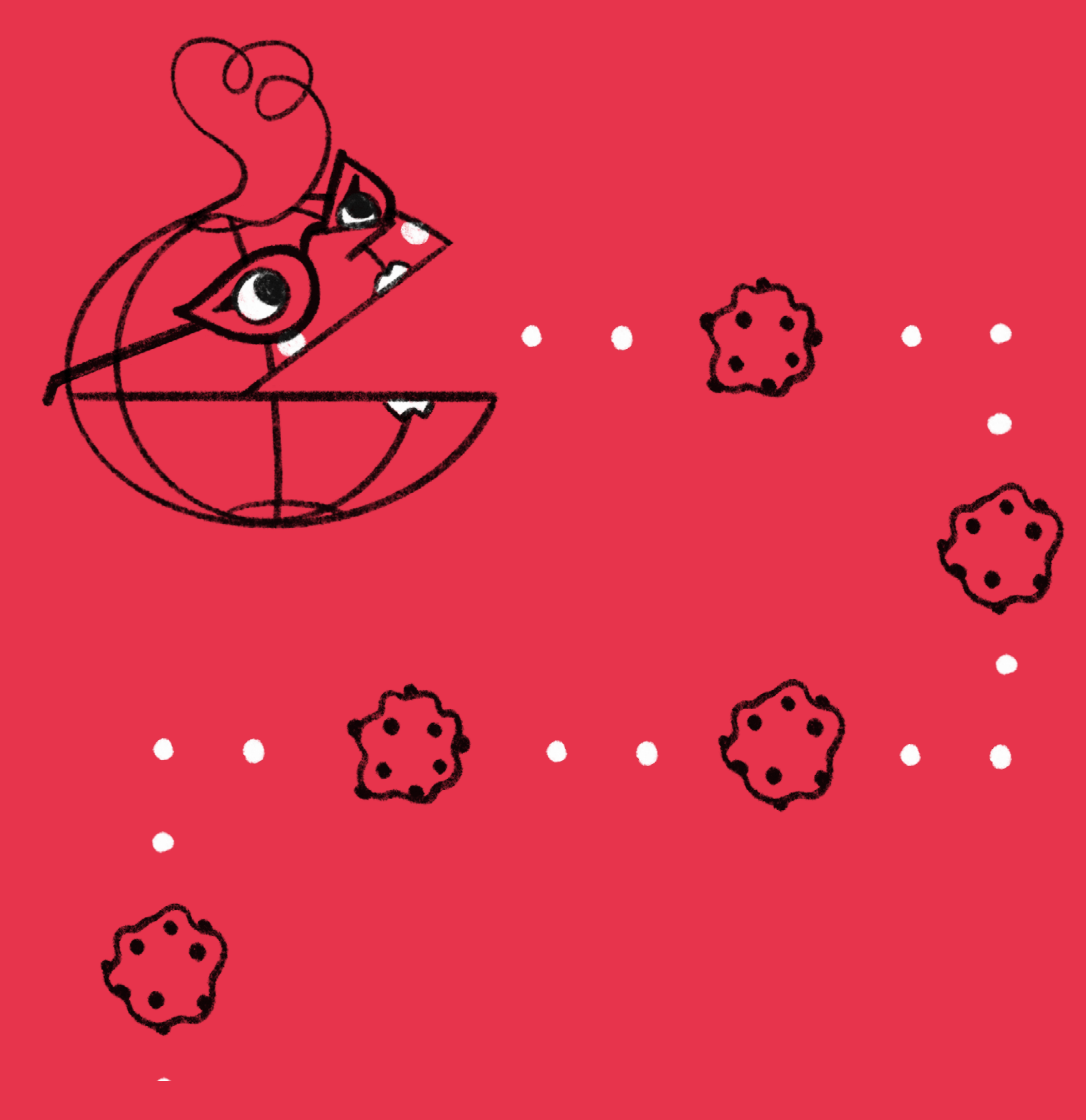
- En naranja, la "cabecera" de la solicitud que incluye los metadatos, la información que describen el paquete que estamos analizando. Cada tipo de metadato va seguido de ":" y luego especifica sus valores. Por ejemplo el metadato "`Cookie`" incluye una *cookie* de identificación de la sesión `PHPSESSID` y las *cookies* de Google Analytics `utma`, `utmb` y `utmz`, entre otras características.

- Finalmente, en rojo, el contenido propiamente dicho del paquete, la información que vamos a transmitir. En este caso las respuestas del formulario que estamos llenando. El nombre `name=Karolina+Uribe`, el correo `email=karolinauribebogota%40gmail.com`, etc.

....

4. Entre las reglas de comunicación en el protocolo http, se encuentran aquellas referidas a cómo nuestros computadores o dispositivos, actuando como clientes, envían las solicitudes al servidor. Para ello existen varios métodos y dos de los más utilizados son los señalados GET y POST. Las diferencias entre ambos se escapan del objetivo de nuestro texto. Sin embargo, sí que es interesante pensar que las solicitudes GET no están pensadas originalmente para enviar información del cliente, más allá de las *cookies*, mientras que las solicitudes POST sí son hechas para enviar información del cliente dirigida a ser inscrita en las bases de datos del servidor. ¿Entonces no se usan solicitudes GET si quiero entrar en una página que requiere mis datos de acceso como mi cuenta de correo? Aquí viene un matiz, las solicitudes GET pueden enviar información del cliente pero únicamente como parte de la URL y no bajo la lógica de inscribir en la base del servidor sino de consultar para identificar. No obstante, esto no es deseable y no es una buena práctica, en términos de seguridad, si implica insertar en la URL datos de identificación con cierta sensibilidad.

Cómo nos siguen por internet. El rastreo web



Con la explicación técnica anterior ya estamos en capacidad de entrar en materia para entender el tema que más nos interesa en este informe, las diferentes técnicas de rastreo que permite identificar a las personas que usan un servicio web (ya sea una página web o una aplicación) y recolectar información sobre ellas y los servicios que utilizan. Esto es lo que se denomina rastreo web o en inglés *web tracking*[1]. En origen, esta práctica tenía dos finalidades importantes para el gestor de una página web: conocer las estadísticas de la misma y poder ofrecer una experiencia adaptada e individualizada a los usuarios. Sin embargo, el paso del tiempo no solo ha supuesto una mejora en las técnicas de rastreo, sino también el descubrimiento de nuevas finalidades para las mismas. Estas nuevas finalidades interesan a otros actores como las empresas de *marketing* digital. Para ellas, el objetivo del rastreo web es poder seguir los intereses y el comportamiento de una persona que usa internet con el fin de tener el mejor conocimiento de ella y estar en capacidad de mostrarle posteriormente la publicidad más adaptada y por lo tanto más eficaz de acuerdo a sus intereses y comportamientos. Esto se hace conociendo los sitios que visita, los artículos que compró, los que no compró pero sí miró, los artículos que lee, sus interacciones en las redes sociales, etc.

Finalmente, una de las clasificaciones de estas técnicas que nos permiten conocer la dificultad de detectarlas es la que diferencia entre técnicas con “cambio de estado” y técnicas “sin cambio de estado”. Así, se separa, respectivamente, entre aquellas técnicas que suponen la instalación de información en nuestro computador, aunque sea de una línea de texto, como las *cookies*, y aquellas técnicas que realizan el rastreo sin afectar localmente nuestro computador, este sería el caso del *fingerprinting*. Entrando ya a las tecnologías, existen muchas y con variantes, por lo que nos centramos aquí en las encontradas en el análisis de las campañas, y que son también parte de las más usadas.

1. Nos referimos aquí a servicios web porque, a pesar de que el contexto que nos resulta más familiar son las páginas web, la misma tecnología se implementa con otros servicios como nuestros correos electrónicos y algunas aplicaciones tanto de computador como de dispositivos móviles. Para esos casos también podemos encontrar algunas técnicas de rastreo.

Cookies (HTTP)

La *cookie*, como tecnología, se inventó en 1994 por parte del equipo de la compañía Netscape para su navegador[2]. El objetivo era volver las páginas web algo más económicamente viable en el mercado ofreciendo una experiencia personalizada. El uso de una *cookie* permitía saber si quien usaba el navegador había visitado con anterioridad una determinada página y se la mostraba de la forma como la había configurado: idioma, ubicación, etc.

Pero ¿qué es una cookie? No es más que una pequeña información que se instala a distancia en nuestros equipos y puede ser leída a distancia por un servidor web. Habitualmente se dice, seguramente por facilidad en la comprensión, que una *cookie* es una archivo de texto, pero esta es solo una de las formas en las que se almacena. Su forma concreta depende del navegador que estemos utilizando. Así, en algunos navegadores se puede almacenar un archivo por cada *cookie*, en otros se crea un sólo archivo cifrado que contiene todas las *cookies* y en otros casos una base de datos en la que cada *cookie* es una entrada.

Si bien las *cookies* fueron inicialmente pensadas y creadas para cumplir con finalidades técnicas (ej: mantener una sesión) o funcionales (ej: mostrar la información en el idioma preferido, o guardar los artículos de una canasta de compra), pronto se empezaron a usar para rastrear a las personas usuarias en un contexto de publicidad dirigida asignando y almacenando un identificador de usuario o creando perfiles de usuario. En cuanto a su contenido, una *cookie* tiene varias características de las cuales las más importantes son: su nombre, su dominio, su contenido, su fecha de expiración o su duración (este puede ir desde el tiempo que dura activa la sesión hasta varios años).

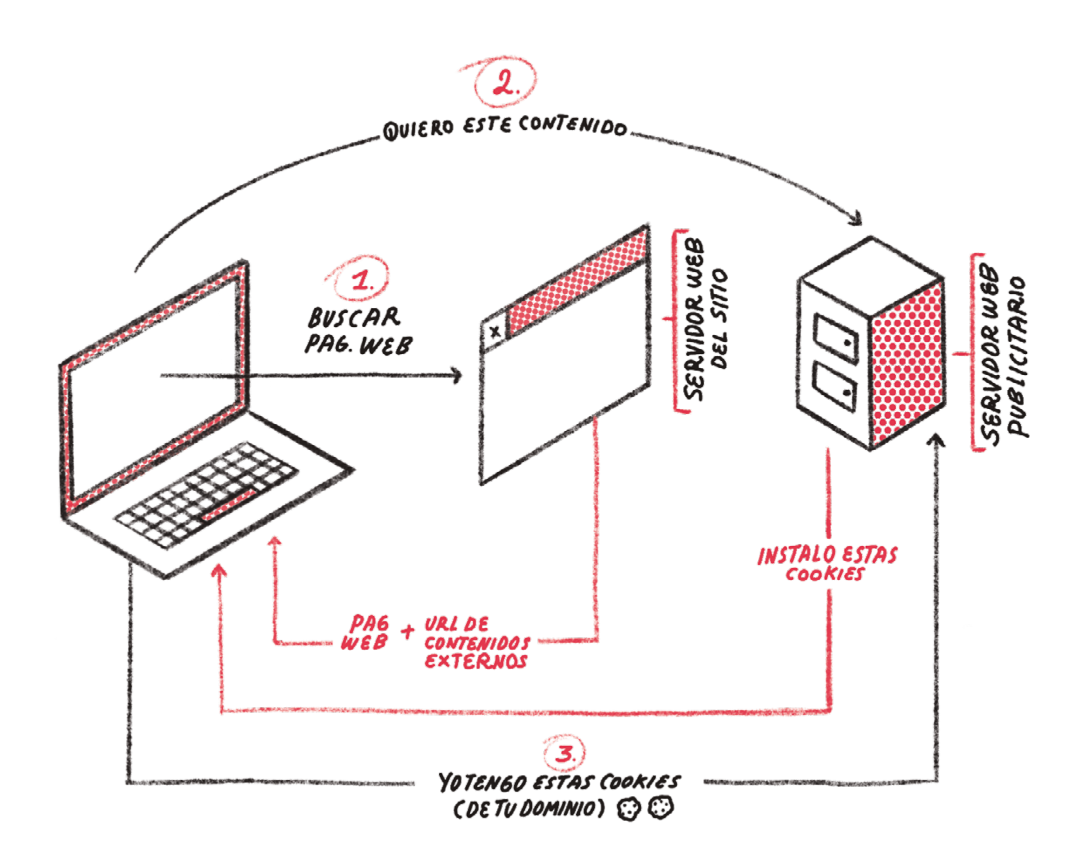
Por otro lado, podemos clasificar las *cookies*[3] tomando en consideración los siguientes criterios:

2. Hay un largo e interesante recorrido en la historia de los navegadores pero la vertiente de la que hablamos nace con Mosaic, cuyos creadores fundaron la empresa Netscape. El primer navegador de Netscape estuvo disponible a finales de 1994 y por años intentó competir con el navegador Internet Explorer de Microsoft. A comienzos de 1997 Netscape liberó el código de la versión 4 de su navegador lo que permitió el desarrollo de Mozilla y posteriormente el surgimiento del Firefox, uno de los navegadores más usados a día de hoy, libre y abierto, desarrollado por la Fundación Mozilla.

3. Esta clasificación es útil a los efectos de explicación, pero las capacidades tecnológicas pueden hacer porosas las categorías con el objetivo de escapar de limitaciones regulatorias.

Si nos centramos en la duración de las mismas, cuánto tiempo van a permanecer escritas en nuestro dispositivo, encontramos:	• **De sesión:** que serán borradas cuando cerremos el navegador o la sesión de la web en cuestión. • **Persistentes:** aquellas que permanecen tras cerrar el navegador y no desaparecerán hasta que el usuario las borre manualmente o caduquen. En este sentido, las *cookies* tienen fecha de expiración, pero, como ya señalamos, este puede ser de años.
Si nos fijamos en la proveniencia de las mismas, tenemos:	• **De origen (*first party*):** instaladas por el servidor de la página web que estamos visitando. Sin embargo, pueden estar también asociadas a servicios externos, como es el caso de *cookies* de Google Analytics que el servidor que visitamos instala para conocer las estadísticas de su página. • **De terceros (*third party*):** instaladas por otros servidores que no son los de la página web que visitamos y que pueden ser leídas por estos terceros. Por ejemplo, un publicista o un sistema de analítica.
Finalmente, por la función de las mismas, las *cookies* pueden ser:	• **Técnicas o funcionales:** aquellas sin las cuales el objeto de la navegación sería imposible o se dificultaría la experiencia de navegación. Sin ellas, por ejemplo, no se podría mantener una conexión autenticada a una cuenta en línea, no podríamos hacer ninguna compra en línea porque el navegador "se olvidaría" de los productos al pasar al proceso de pago o al seguir buscando otros para añadir a la canasta. Incluye también aquellas que adaptan la experiencia a nuestras preferencias como el idioma en que aparece google.com o el hecho de que el clima que se nos ofrezca sea el de la ciudad en que estemos sin necesidad de indicarlo previamente. • **Estadísticas o de rendimiento:** aquellas que recopilan información sobre cómo se está utilizando la web para mejorar su funcionamiento. No permiten la identificación del usuario y, si son de terceros, responden a servicios de analítica dirigidos a la mejora de la web. • **De *marketing*:** aquellas que tienen como finalidad o parte de sus finalidades adaptar la publicidad que se recibe a través de internet para que sea más relevante para la persona usuaria. Suelen ser de terceros y son las que más fácilmente circulan entre distintos actores.

A los efectos de rastreo, nos interesa conocer un poco más de las *cookies* de terceros. Esta clasificación solamente se refiere a la proveniencia de la *cookie*, independiente de cómo se instala, cómo se almacena o cómo se lee. Es decir, a menos que activamente hagamos algo, nuestro computador se comportará de igual manera con las *cookies* de terceros o con las de origen, no las distingue. ¿Qué ocurre entonces? Que cuando nuestro computador se conecta a un servidor solicitando la página web que deseamos, le envía a este las *cookies* relacionadas con dicha página. Pero si entre ellas también se encuentran *cookies* de servidores terceros, se la enviará también a estos con nuestro identificador.



¿Y qué problema tiene esto? Que existen compañías que van acumulando información de nuestra navegación y uso de distintos servicios web, esto es el denominado el rastreo entre sitios web o *cross-site tracking* en inglés[4]. Pongamos un ejemplo pensemos ¿qué sabe YouTube de nosotros? Conoce los vídeos que vemos en su página, pero también sabe lo que vemos en otras páginas o en las redes sociales y con eso nos ofrece sugerencias más específicas. Pero YouTube pertenece a Google, que desarrolla el navegador de uso común *Chrome*, pero también sabe cómo interactuamos con distintas páginas que utilizan sus servicios de estadística, *Google Analytics* o los de *marketing*, *Google Ads*. Es decir, Google sabe mucho de nosotros. En realidad el problema es que es muy difícil saber cuánto sabe Google de nosotros[5].

El píxel de rastreo (o web bug)

La técnica del pixel[6] de rastreo se construye sobre lo que ya conocemos sobre lenguaje HTML y que se encuentra detrás de una página web. Se inserta un pequeño tag en la forma de una imagen, casi siempre transparente, de un tamaño máximo de 1 x 1 píxeles. Siendo así, el usuario no percibe nada mientras navega por la página o lee el correo electrónico. Sin embargo, que no lo veamos no impide que nuestro computador lo lea y ejecute como parte del código, realizando una solicitud al servidor, distinto al que nos provee la página y la mayoría de las veces de *marketing*, para obtener la “imagen”. Podemos decir que, en cierta forma, el pixel de rastreo actúa donde se ubica esta supuesta imagen externa. Al hacerlo, el navegador del usuario va a solicitar esta imagen al servidor externo, iniciando una comunicación HTTP(S) entre el navegador del usuario y el servidor web publicitario, en paralelo de la conexión con el servidor web principal (en el caso de nuestro estudio, el del candidato). Al hacer esto, va a transmitir información al servidor externo publicitario, como la dirección IP del usuario, las características su equipo, las eventuales *cookies* instaladas por el dominio, etc. En respuesta a esta solicitud, el servidor web externo puede, además, instalar una o varias *cookies* en nuestro computador.

En ciertos casos —en particular para los correos electrónicos— el nombre de la imagen ficticia o sus parámetros hay un número de identificación o informaciones personales del usuario. Esto permite saber quién abrió el correo o visitó la página y eventualmente combinarlo con otras técnicas de rastreo como el *fingerprinting*, que trataremos más adelante.

En cuanto a la forma de esta técnica, este es un ejemplo de línea de código que se encontraría dentro del cuerpo de la página o el correo electrónico:

4. En realidad, el *cross-site tracking* se realiza con más herramientas de rastreo, pero creemos que hablando de *cookies* de terceros es un buen momento para introducirlo por ser una de sus principales problemáticas.

5. Actualmente Google sí permite que sepamos qué datos tienen vinculados a nuestra cuenta de correo y nos permite descargar la información. Esto se puede hacer en https://takeout.google.com/. Sin embargo, permite descargar la información vinculada a un correo, que no es necesariamente toda la información que tiene. Por otro lado, no todos las empresas que acumulan datos nuestros nos dan este tipo de posibilidad.

6. El píxel es la unidad mínima de color en una imagen digital, un cuadro de un mismo color. Las imágenes digitales se componen de la unión de estos cuadros. Por eso, según ampliamos una imagen en nuestra pantalla, podemos encontrar que se empiezan a distinguir esos cuadros (en jerga se le dice a la imagen que “está pixelada”, que no es más que señalar que se ven los píxeles). Cuando hablamos de resolución, como indicador de la calidad y detalle de la imagen, no estamos más que refiriéndonos a los píxeles de la misma, ya sea indicando directamente los píxeles a lo ancho y a lo alto (cuando hablamos de resolución de pantalla, por ejemplo 640 x 480) o el resultado de multiplicarlos (cuando hablamos de resolución de una cámara, por ejemplo 5 megapíxeles que se obtiene de redondear 2.560 [ancho] x 1.920 [alto] = 4.915.200 píxeles).

```
<img src = http://tracking-y-marketing.com/pixel.png?user_
id=52ab5ec6200ab788&email=karolinauribe@gmail.com width=0 heigth=0>
```

El código `img` le señala a nuestro navegador que va a mostrar una imagen, mientras `src=` señala la fuente (*source*) de la misma, que iría luego del =. Al ejecutar esta porción de código HTML, nuestro navegador va a iniciar una comunicación con el servidor `tracking-y-marketing.com` para solicitarle la imagen ficticia `pixel.png` de tamaño 0 (`width=0 heigth=0`). En el mismo acto, le transmite el número de identificación (`user_id=`) y el correo electrónico (`email=`) del usuario.

Fingerprinting

Imaginemos que usted es el único mercado de la ciudad pero que interactuamos solo por teléfono.

Un día le pido unos zapatos, para ello le doy mi talla. Resulta que soy miope, así que le doy mi graduación para que me haga unas gafas. Igualmente, le pido ropa y le voy dando tallajes. Pero quiero escribir este texto, así que le pido un computador con unas características. ¿Van viendo a dónde vamos a llegar? Después de unas cuantas interacciones, no solo sabrá cómo soy físicamente, sino también cómo me gusta vestir, cómo está más o menos configurado mi espacio de trabajo… Y nunca me ha visto. Esta es la misma lógica que subyace al *fingerprinting*: adicionando de manera lógica ciertas piezas de información que en sí mismas pueden parecer inocuas, podemos obtener identidades únicas.

Siendo un poco más técnicos, el *fingerprinting* permite obtener y combinar a distancia la información de ciertas características técnicas de nuestro dispositivo como el modelo, la versión del sistema operativo y del navegador o la resolución de pantalla, de manera pasiva o activa. La obtención y combinación de esta información permite construir una huella digital única o casi única de nuestro equipo con el fin de identificarlo en sucesivas conexiones, lo que permite nuestro rastreo. ¿Imposible?, veámoslo:

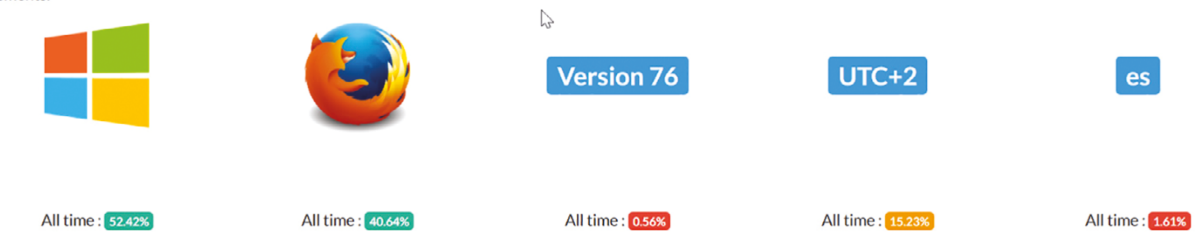
> Esta es una captura de la web https://amiunique.org. Aparecen los porcentajes de navegadores que muestran las mismas características que el mío. Recogemos aquí parte del resultado, pero las características cruzadas para obtener un perfil único son más.

My browser fingerprint

Are you unique?

All time : Yes! (You can be tracked!)

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.



All time : However, your full fingerprint is unique among the 2065703 collected so far.

Podemos considerar el *fingerprinting* problemático en términos de privacidad porque presenta al menos dos cuestiones que se relacionan con el hecho de ser una técnica de rastreo “sin cambio de estado”:

1. El uso de esta tecnología es casi indetectable incluso para un especialista. Dicho de otra manera, el *fingerprinting* es una técnica de rastreo furtiva. Esto complica el hacer efectiva la normativa de protección de datos.

2. En general es muy difícil bloquear el *fingerprinting*. Un bloqueo de las *cookies* o incluso un modo de navegación privada o una limpieza del historial de navegación no protege contra el *fingerprinting*.

Hasta aquí…

- Nos hemos acercado a la práctica del rastreo web y a una primera clasificación con gran impacto en la posibilidad de detectarlo en razón de si suponen un cambio de estado o no.
- Hemos conocido las *cookies*, sus tipos y la problemática de las *cookies* de terceros.
- Nos hemos aproximado al píxel de rastreo y cómo se nos escapa a primera vista.
- Hemos aprendido que somos únicos en nuestra navegación y que de eso se sirve el *fingerprinting*.

El uso de rastreo web en las candidaturas a la alcaldía

Pasemos a ver entonces qué herramientas de rastreo han utilizado los candidatos a la Alcaldía. Comenzamos viendo las *cookies* que aparecen en relación a cada uno de los 4 sitios web principales de los candidatos: el número de *cookies* instalados, sus tipos y los dominios asociados.

CLAUDIA LOPEZ
www.claudia-lopez.com

- de origen, incluyendo sevicios de Shopify y *Google Analytics*,
- esconelverde.com: dominio del partido político de Claudia Lopez,
- zdassets.com y zopim.com: CHAT de la empresa Zendesk,
- beeapp.me: servicio de contacto por WhatsApp
- dawtemplatesmaster.com: lector audio,
- soundcloud.com: lector audio,
- facebook.com,
- youtube.com,
- doubleclick.net: publicidad de Google (*causado por el uso de YouTube*)

CARLOS FERNANDO GALÁN
www.bogotaparalagente.com

- de origen, incluyendo *Google Analytics*,
- YouTube,
- doubleclick.net: publicidad de Google (*causado por el uso de YouTube*)

HOLLMAN MORRIS www.hollmanmorris.co	• de origen, incluyendo *Google Analytics*, • YouTube, • doubleclick.net: publicidad de Google (c*ausado por el uso de YouTube*)
MIGUEL URIBE TURBAY www.migueluribeturbay.co	• de origen, incluyendo Google Analytics y Mautic (*marketing*/publicidad), • navdmp.com: marketing online/publicidad (Navegg DMP) • messengerpeople.com: servicio de contacto (vía servicios de mensajerías externa como WhatsApp y Facebook Messenger) • toutube.com • doubleclick.net: publicidad de Google

Aunque no es el caso para todas las *cookies*, en el ejemplo de elección a la Alcaldía, todas las *cookies* que encontramos se instalan apenas el usuario llega a la página. Incluso en los sitios de Claudia López y Miguel Uribe Turbay, en los cuales hay una banda de información/consentimiento para las *cookies*, respectivamente con un botón "Aceptar" y "Lo entiendo". La presencia de esas bandas de consentimiento sugeriría que la instalación de las *cookies* es posterior a la aceptación de la misma. Pero no es así en este caso: las *cookies* ya se instalan antes de aceptar/rechazar la banda de consentimiento de las mismas. En relación a lo que hablamos del *cross-tracking*, si varios sitios web han puesto *tags* de la misma empresa publicitaria (ej: Google), las *cookies* de esta empresa le permitirán conocer, entre otros datos, el hecho de que hemos navegado por dichos sitios. Es decir, puede

que Miguel Uribe Turbay no sepa que he navegado por la web de Carlos F. Galán, pero la empresa tercera sí.

Ahora, ¿y cómo es una *cookie* "por dentro"? Para visualizar las *cookies* nosotros usamos la extensión de navegador de código abierto llamado *Cookie Manager* +. Esta herramienta permite visualizar ciertas características de las *cookies* en columna o exportar las *cookies* completas en formato de texto. Aquí está como ejemplo la *cookie* de rastreo "IDE" de Google del dominio "doubleclick.net", instalada desde el sitio web de Miguel Uribe Turbay:


```
Host:                   .doubleclick.net
Host raw:               .doubleclick.net
Name:                   IDE
Name raw:               IDE
Path:                   /
Path raw:               /
Content:
AHWqTUl7Mk1jLPH-Q88F1MNzA7WxKWmRpJy-qm4oTdsziKx03Qb9o1vh-I8fXmwg
Content raw:
AHWqTUl7Mk1jLPH-Q88F1MNzA7WxKWmRpJy-qm4oTdsziKx03Qb9o1vh-I8fXmwg
Expires:                14 de septiembre de 2021 18:50:56 GMT-5
Expires raw:            1631663456
Send for:               Cualquier tipo de conexión
Send for raw:           false
Created:                15 de septiembre de 2019 18:50:57 GMT-5
Created raw:            1568591456550132
Last accessed:          15 de septiembre de 2019 18:50:57 GMT-5
Last accessed raw:      1568591456550132
HTTP only:              Yes
HTTP only raw:          true
This domain only:       Yes
This domain only raw: true
Policy:                 no information available
Policy raw:             0
Status:                 no information available
Status raw:             0
originAttributes: {"appId":0, "firstPartyDomain":"",
"inIsolatedMozBrowser":false,"privateBrowsingId":0,"userContextId":0}
```

Uso de herramientas publicitarias en el sitio de miguel uribe turbay

¿Recuerdan cuándo hablamos de que es útil conocer en qué servidores están los sitios web? En la tabla que mostramos de los candidatos, se muestra que el sitio web de Claudia López está alojado en servidores de una empresa llamada Shopify. Como se puede deducir también del nombre, esta provee soluciones integradas de *marketing* en línea. Y esto nos lleva a preguntarnos ¿estará usando la candidata dichas soluciones? Cruzando análisis basados en todos los conceptos aprendidos hasta ahora (HTML: estudio del código fuente; HTTP: análisis de los flujos de datos; rastreo: revisión de las *cookies*) confirmamos el uso de estas soluciones.

En el código fuente de la página de inicio del sitio de Claudia López, aparece una herramienta de *remarketing* de Shopify a través de campañas en Google y Facebook llamada "ROI Hunter Easy"[7] (ver anexo "Uso de la herramienta ROI Hunter Easy en el sitio de Claudia López"). El *remarketing*, a veces llamado también *retargeting*, consiste en mostrar un anuncio sobre algún tema en relación al cual el usuario ya ha manifestado un interés, ya sea en sitios de anunciantes o en otros contextos (ej: Facebook, YouTube). En el caso de un sitio político como el sitio de Claudia López, esto supone que se podría mostrar publicidad de su campaña en otros sitios web tras "haber manifestado un interés" por medio de la visita a su sitio web o empezando o terminando el proceso de registro.

7. En la página de la propia empresa podemos encontrar más información al respecto de dicha solución de *marketing*: https://apps.shopify.com/roi-hunter-easy?locale=es

Para finalizar este capítulo de rastreo, mostraremos un caso de análisis completo a través del ejemplo del sitio de Miguel Uribe Turbay. Hemos elegido este por ser el que más tiene para mostrar en este sentido. Comenzando con el análisis del código fuente, de las *cookies* y de los flujos HTTP(S), encontramos el uso de las siguientes tres herramientas de publicidad (ver anexo "Herramientas *marketing* y rastreo en el sitio de la campaña de Miguel Uribe Turbay"):

1. Mautic,
2. Navegg DMP (dominio "navdmp.com"),
3. El servicio *marketing* de Google (dominio "doubleclick.net").

Mautic - *Modern Marketing Automation*: es una herramienta de la empresa Acquia que permite adaptar dinámicamente el contenido del sitio web y de las campañas de publicidad desde una perspectiva multicanal y en función de la audiencia[8]. El aspecto "multicanal" se verificará más adelante en al análisis de los correos electrónicos recibidos.

Una particularidad asociada al uso de Mautic que resalta en el análisis técnico del sitio web es la utilización de un subdominio con nombre explícito: "marketing.migueluribeturbay.co" que corresponde, como vimos más arriba, a un servidor web distinto del dominio principal[9].

8. El sitio de la empresa Acquia ofrece, en inglés, la siguiente descripción: "*Mautic is a fully-featured marketing automation platform that enables organizations of all sizes to send multi-channel communications at scale, and simultaneously personalize the experience for individual contacts. Mautic helps teams gather important contact information, optimize and replicate campaigns, and ultimately, report on results*.", https://www.acquia.com/products-services/mautic

9. Vimos arriba que, tienen direcciones IP distintas. Además, el análisis de las respuestas HTTP(S) del servidor web muestra que es de tipo "Apache/2.4.29 (Ubuntu)" mientras el servidor web del dominio principal es de tipo "NGINX".

Un análisis de las *cookies* instaladas muestra que las asociadas a este subdominio, relacionadas con las herramientas de Mautic, son instaladas apenas un usuario llega en la página web principal del candidato. A pesar de ser utilizadas por el mismo candidato, han de considerarse *cookies* de terceros por provenir de un dominio distinto, como podemos ver en la siguiente captura.

	Domain	Name	Content
☐	.migueluribeturbay.co	_gid	GA1.2.660391297.1568591455
☐	marketing.migueluribeturbay.co	mautic_device_id	a6vug7i9r3qtgqzss97v806
☐	marketing.migueluribeturbay.co	mtc_id	56206
☐	marketing.migueluribeturbay.co	mtc_sid	a6vug7i9r3qtgqzss97v806
☐	marketing.migueluribeturbay.co	mautic_session_id	a6vug7i9r3qtgqzss97v806
☐	marketing.migueluribeturbay.co	a6vug7i9r3qtgqzss…	56206
☐	marketing.migueluribeturbay.co	mautic_referer_id	85166

Por su parte, **"DMP" (*Data Management Platform*)**, de la empresa brasileña Navegg, es una solución para las agencias de publicidad y los anunciantes que permite, según lo señalado por la propia empresa en su sitio, realizar la gestión de datos, la segmentación de audiencia y la "activación" de esta audiencia vía campañas de publicidad[10]. Esto incluye la publicidad de tipo *retargeting* pero también exploración de nuevas audiencias posibles (lo que se llama *lookalike*) y otro tipo de estrategias *marketing*. Quizás el hecho de que hayan aparecido publicidades de Miguel Uribe desde distintos perfiles de navegación (ver siguiente capítulo, Ciudadana Virtual) tiene que ver con el uso de esta funcionalidad.

Por fin, la presencia de las *cookies* de Google/Doubleclick se debe al uso de servicios publicitarios de Google que permiten mostrar publicidades relacionadas en otros sitios o proponer vínculos esponsorizados cuando alguien hace búsquedas vía Google[11]. Esto se puede ver en más detalle en el anexo "Instalación de la *cookie* de Doubleclick en el sitio de la campaña de Miguel Uribe Turbay".

Otra de las características en el caso del candidato Miguel Uribe Turbay fue el uso de *fingerprinting*. Pese a estar relacionado con el uso de Mautic, el

……………………………….

10. https://www.navegg.com/es/soluciones/dmp-agencias-anunciantes/

11. https://ads.google.com/intl/es_CO/home/

fingerprinting merece una presentación autónoma por ser sustancialmente distinto a hallazgos previos y debido a sus implicaciones en términos de privacidad y consentimiento.

Logramos detectar el uso de *fingerprinting* en el sitio web de Miguel Uribe Turbay vía el análisis de flujo HTTP(S). Detectamos un paquete HTTPS que tenía una variable explícitamente denominada `fingerprint` en los parámetros de su URL, junto con una serie de características técnicas del computador:

```
https://marketing.migueluribeturbay.co/mtracking.gif?page_title=Inicio%20%7C%20
Miguel%20Uribe%20Turbay&page_language=es-CL&page_referrer=www.migueluribeturbay.
co&page_url=https%3A%2F%2Fwww.migueluribeturbay.co%2F%3Fcn-reloaded%3D1&coun
ter=0&resolution=1280x720&timezone_offset=300&platform=Linux%20x86_64&do_not_
track=unspecified&adblock=false&fingerprint=8785309d593003dc0221dd48f037a5b9
```

```
GET /mtracking.gif?page_title=Inicio%20%7C%20Miguel%20Uribe%20
Turbay&page_language=es-CL&page_referrer=www.migueluribeturbay.co&page_
url=https%3A%2F%2Fwww.migueluribeturbay.co%2F%3Fcn-reloaded%3D1&counter=0
&resolution=1280x720&timezone_offset=300&platform=Linux%20x86_64&do_not_
track=unspecified&adblock=false&fingerprint=8785309d593003dc0221dd48f037a5b9 HTTP/1.1
```

Si bien en el anexo "Uso de técnicas de *fingerprinting* en el sitio de la campaña de Miguel Uribe Turbay" se encuentra mayor información, podemos ya aplicar algunas de las cosas aprendidas:

- La variable `fingerprint` contiene un identificador. Posiblemente, ese sea el modo de rastrear nuestro equipo.
- Se utiliza el método GET para solicitar un pixel de rastreo con nombre explícito (`mtracking.gif`), por lo que, si se envía información del cliente se hace en la propia URL[12]. Así es en este caso, como se ve en la información destacada en rojo: la resolución de nuestro navegador - `resolution=`, la zona horaria - `timezone_offset=`, el sistema operativo - `platform=` y el uso de herramientas para bloquear el rastreo - `do_not_track=`.

12. Ver arriba capítulo "Caminando por el mapa de internet", nota 4

Además del análisis, buscamos en la documentación técnica de la herramienta de Mautic y encontramos una descripción de la funcionalidad de *fingerprint*, todavía en versión Beta, en una página titulada "Contact Monitoring" (monitoreo de los contactos)[13].

Dos puntos importantes de esta documentación resaltan:

1. La implementación del *fingerprint* no resulta de un uso por defecto de la solución Mautic sino de una parametrización activa por parte de quien lo administra. En otras palabras, los que administraban el sitio web de Miguel Uribe Turbay decidieron usar el *fingerprint*.

2. La documentación técnica describe explícitamente que el objetivo de la herramienta es poder seguir rastreando a un usuario que bloquea las *cookies*, ya que sin esa herramienta sería visto como un usuario nuevo[14]. Es decir, el uso por parte del candidato está dirigido a rastrear a los usuarios a pesar de que hayan tomado acciones en contra de ello como el bloqueo de *cookies*.

Finalmente y para completar la lista de técnicas de rastreo, Miguel Uribe Turbay utilizó también el píxel de rastreo en sus correos electrónicos. Recordemos que, al estar basados en la misma tecnología, podemos hacer los mismos análisis. De esta manera, al realizar una captura de los flujos HTTP(S) producidos por la apertura del primer correo recibido tras la inscripción a través del formulario de su web, detectamos el uso de esta herramienta.

13. https://www.mautic.org/docs/en/contacts/contact_monitoring.html

14. "Note that if a browser is set to not accept cookies, this may result in each hit creating a new visitor. If this behavior is concerning, see Fingerprint option below [...] Mautic 1.4.0 comes with a tracking feature called fingerprint. Fingerprint2 library was used. It should work together or replace current tracking identifiers like IP address and/or cookie ID."

Primer correo electrónico recibido de la campaña de Miguel Uribe Turbay

From Avancemos Miguel Uribe <no-reply@marketing.migueluribeturbay.co>

Subject **Bienvenido al equipo de Miguel Uribe**

To Me <karolinauribebogota@gmail.com>



Hola Karolina Uribe

Bienvenido a nuestro equipo. **Bogotá se juega mucho en las próximas elecciones**. Se nos presentan dos opciones: retroceder, a la época de la parálisis, la negligencia y la corrupción, o avanzar, con inteligencia, con hechos concretos y sin carreta, para construir una ciudad segura, sostenible e inteligente.

Si queremos avanzar, es fundamental trabajar juntos, en equipo. Para eso necesito de tu ayuda, vuélvete vocero de esta causa. Cuéntale a tu familia, a tus amigos y conocidos de nuestro mensaje. Conviértete en un multiplicador de **#Avancemos**.

Basta del populismo, basta de la carreta. Vamos a demostrar que la confianza de los bogotanos se recupera con hechos concretos, con obras, con trabajo y con disciplina. Como tú, amo Bogotá y trabajaré incansablemente para que nuestra ciudad avance.

Un gran abrazo,

Miguel Uribe Turbay



Extracto de la captura HTTP(S) de la solicitud de nuestro equipo al abrirlo

```
https://marketing.migueluribeturbay.co/
email/5d884ca28dbb2664034033.gif

GET /email/5d884ca28dbb2664034033.gif HTTP/1.1
Host: marketing.migueluribeturbay.co
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Cookie: nvg56903=9da5f54b64b0b63c54f9ee57f09|2_266; _
ga=GA1.2.1048251503.1569213115; _gid=GA1.2.2074022322.1569213115;
__utma=21743527.1048251503.1569213115.1569213121.1569213121.1; __
utmb=21743527.4.9.1569213360418; __utmz=21743527.1569213121.1.1.
utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: keep-alive
```

Extracto de la captura HTTP(S) de la respuesta del servidor

```
HTTP/1.1 200 OK
Date: Mon, 23 Sep 2019 04:59:11 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie:
539f581af2ac98b32c119d8ef1881172=pfb3jm0l354f28aos07i1rnhod;
path=/; secure; HttpOnly
Set-Cookie: mautic_session_id=deleted; expires=Thu, 01-
Jan-1970 00:00:01 GMT; Max-Age=0; path=/; secure
Set-Cookie: mautic_device_id=mo9416cnwfdrp6vk1o252wr; expires=Tue,
22-Sep-2020 04:59:11 GMT; Max-Age=31536000; path=/; secure
Set-Cookie: mtc_id=65300; path=/; secure
Set-Cookie: mtc_sid=mo9416cnwfdrp6vk1o252wr; path=/; secure
Set-Cookie: mautic_session_id=mo9416cnwfdrp6vk1o252wr; expires=Tue,
22-Sep-2020 04:59:11 GMT; Max-Age=31536000; path=/; secure
Set-Cookie: mo9416cnwfdrp6vk1o252wr=65300; expires=Tue, 22-
Sep-2020 04:59:11 GMT; Max-Age=31536000; path=/; secure
[...]
```

Se puede observar hacia el subdominio “marketing.migueluribeturbay.co” una solicitud de una imagen (5d884ca28dbb2664034033.gif) que sirve para transmitir el número de identificación del usuario en la base de datos *marketing*. Por su parte, el servidor responde instalando 6 *cookies* mediante una serie de instrucciones `Set-Cookie:`. Al menos 4 son asociadas al servicio Mautic y tres de ellas contienen una serie de caracteres alfanuméricos que muy probablemente constituyen un número de rastreo del usuario, permitiendo así su identificación en su navegación ulterior.

Presentando a la ciudadana virtual



Vista la tecnología principal detrás de las relaciones digitales entre la ciudadanía y las campañas políticas, es momento de ver la otra cara de la moneda. Es decir, ¿qué recibimos la ciudadanía como resultado del uso de estas tecnologías? Para saberlo, creamos una "ciudadana virtual" por cada candidatura, así como una que no se relacionaría con ninguna. Cada ciudadana, con excepción de la última, navegaría por la web de la candidatura, se inscribiría en el formulario que hubiera en el sitio y, en caso de que existieran, interactuarían por WhatsApp. Para ello, cada una de las ciudadanas contaría con:

- Nombre y apellidos
- Cédula
- Correo electrónico
- Redes sociales: Twitter y Facebook
- Número de teléfono vinculado a WhatsApp

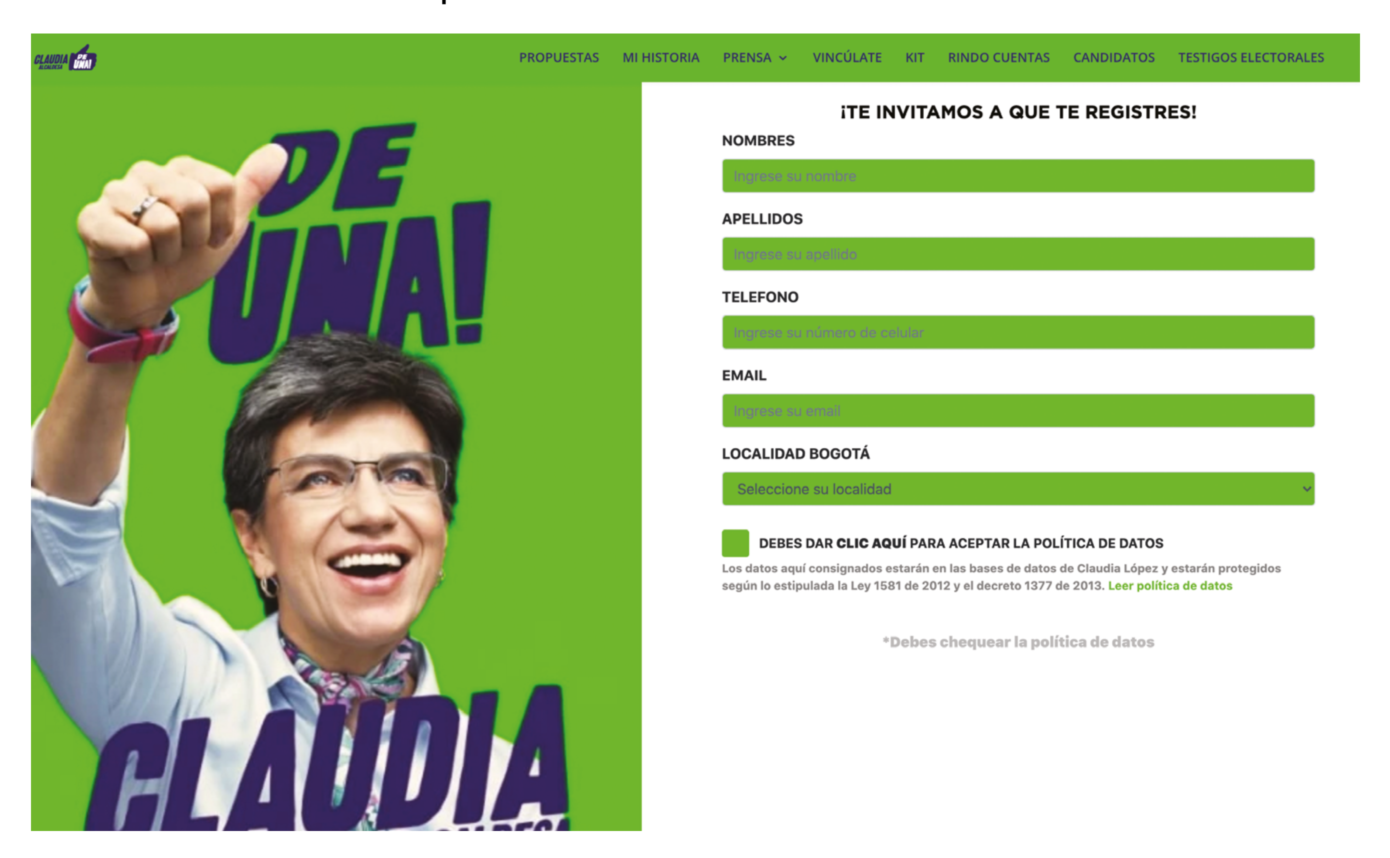
Cada uno de los sitios tenía un formulario de recolección de datos personales que, en relación a la seguridad de la transmisión de los datos, usan todos HTTPS. Respectivamente, se solicitaban los datos siguientes:

- en el formulario "*Te invitamos a que te registres*", del sitio web de **Claudia López**: nombres, apellidos, teléfonos, correo electrónico y localidad de Bogotá. El sitio web de Claudia López contaba también con un formulario de donación en línea que no fue posible analizar al mismo nivel de detalle[1];
- en el formulario "*Voluntarios*"[2] del sitio web de **Carlos Fernando Galán**: nombres, apellidos, lugar de votación, correo electrónico, celular, cédula, temas para enterarse y aportar, localidades de interés y apoyo día elección (testigo electoral, testigo comisión escrutadora, ninguno);
- en el formulario "*Súmate a la Bogotá progresista / Acompáñame*" del sitio web de **Hollman Morris**: nombre, apellido, correo electrónico, teléfono, localidad y organización (los dos últimos, opcionales) ;
- en el formulario "*Si compartes nuestra causa… ¡Únete!*", del sitio web de **Miguel Uribe Turbay**: nombre, correo electrónico y celular.

1. Un análisis real y completo de los flujos de datos, como lo hicimos para otros formulario, habría requerido la realización de una donación en línea y la aportación de datos bancarios.

2. El texto que aparece como subtítulo es "Si quieres sumarte a este movimiento y ayudarnos desde ya a construir un Bogotá Para La Gente, inscríbete aquí:" .

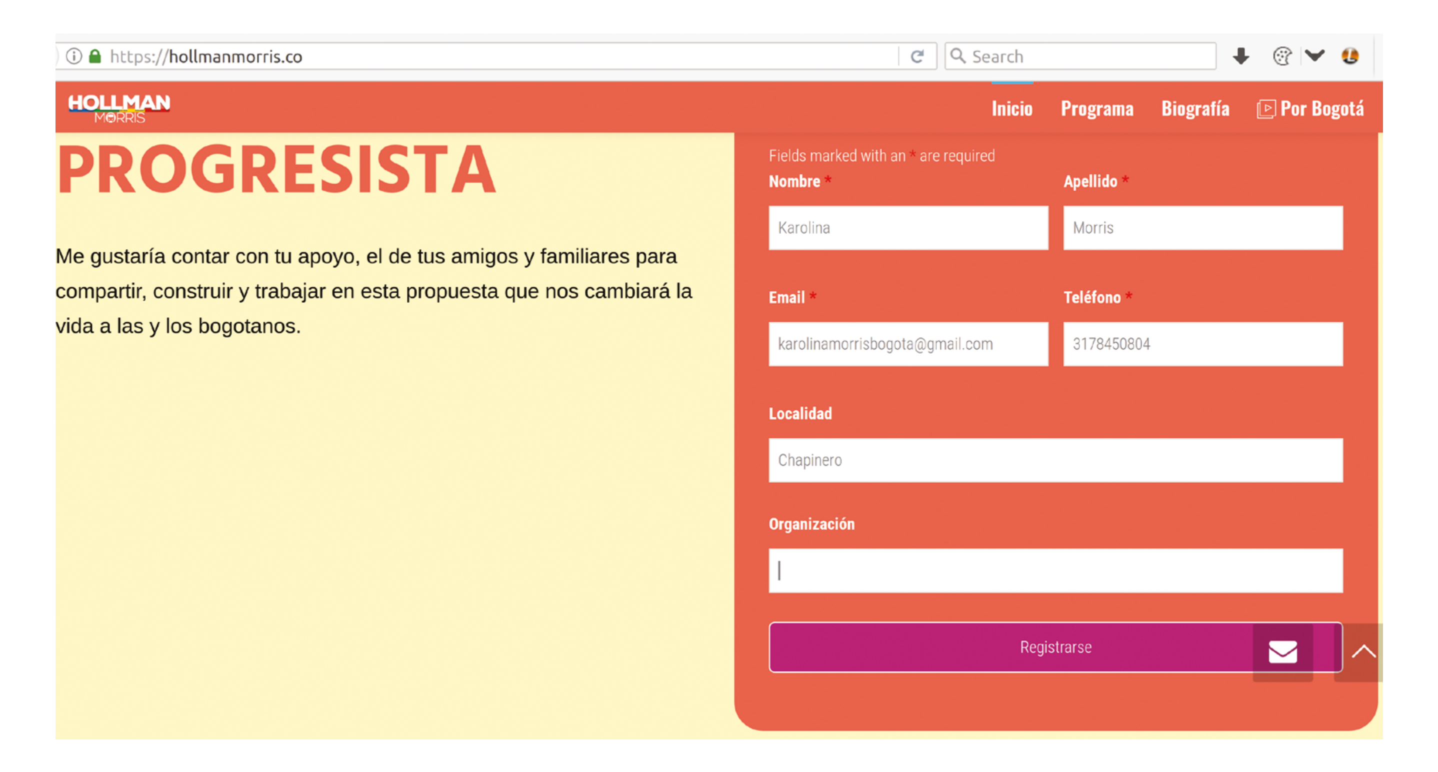
Formulario - Sitio web de Claudia López



Formulario - Sitio web de Carlos F. Galán



Formulario - Sitio web de Hollman Morris



Formulario - Sitio web de Miguel Uribe Turbay



Para observar si las interacciones con los sitios web se traducen en publicidad relacionada con las campañas en nuestra navegación habitual, nos dirigimos a sitios de medios de comunicación colombianos que suelen alquilar espacios publicitarios poco antes de las elecciones del 27 de octubre del 2019. En cuatro de los sitios visitados (Caracol, Semana, El Tiempo y Publimetro) no se observaron impresiones publicitarias relacionadas. En cambio, en La FM y El Heraldo, obtuvimos publicidades relacionadas con las campañas de los candidatos Claudia López y Miguel Uribe Turbay.

Desde ninguno de los perfiles se observaron mensajes publicitarios asociados con las campañas políticas de los candidatos Hollman Morris o Carlos Fernando Galán, lo que concuerda con la ausencia de herramientas de *marketing* en sus sitios web.

Los anuncios publicitarios relacionados con la candidata Claudia López, u otros candidatos en apoyo de su campaña, sólo se observaron desde el perfil de navegación de nuestra ciudadana virtual "***Karolina Lopez***", que manifiesto interés en Claudia López navegando en su sitio y, posteriormente, inscribiéndose al mismo[3]. Por otro lado, los perfiles de las otras ciudadanas virtuales no generaron impresiones de publicidad relacionada con la candidata Claudia López. Esto apunta al uso de herramientas de publicidad dirigida de *retargeting*.

3. Se hicieron estos dos análisis en días distintos. Primero el 9 de septiembre se realizó una visita de la página de Claudia López, con los análisis técnicos correspondiente. Segundo, el 22 de septiembre, inscribimos a nuestra ciudadana virtual "Karolina López" a través del formulario web del sitio.

Captura de pantalla donde se ve un anuncio para votar por Julián Espinosa, de la lista de Claudia López, en el sitio lafm.co



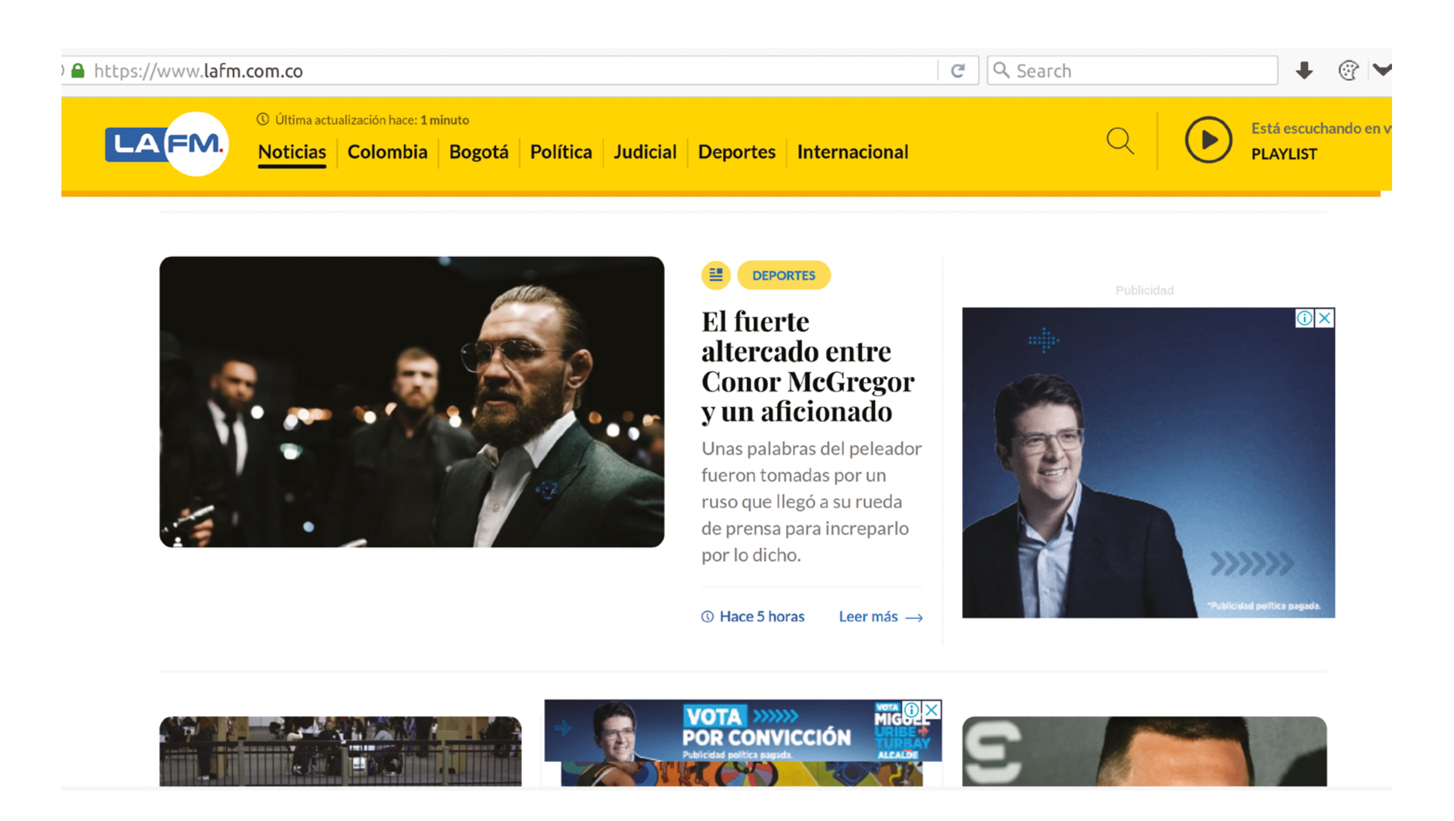
Al hacer clic en el "i" de la información de la publicidad, se pudo comprobar que es un anuncio de Google basado en los sitios visitados o los intereses estimados por Google (en este caso, en el papel de empresa de publicidad)



Esto, con los demás análisis que hemos ido viendo, muestra que es posible que para Claudia López y los candidatos de su lista se hiciera uso de campañas de publicidad dirigida realizadas por Google, recurriendo como intermedio a la mencionada Shopify. Nuestro análisis no permite medir la amplitud de esta campaña, sólo constatar el uso de estas herramientas y su efecto.

Distinto es el caso de impresiones publicitarias relacionadas con el candidato Miguel Uribe Turbay, que fueron obtenidas desde todos los perfiles de navegación, incluso desde el de "Karolina López", que mostró interés por Claudia López, aunque éstas también se tratan de publicidades impresas por Google:

Captura de pantalla donde se ve un anuncio para votar por Miguel Uribe Turbay en el sitio lafm.co



Sin embargo, la información entregada por Google en relación a los motivos de la impresión de la publicidad de Miguel Uribe no es la misma que para la publicidad de Claudia López. En este sentido, incluye "factores generales" acordados por el anunciante y el sitio desde el que se publica, así como información recolectada por el mismo sitio.

Google Why this ad?

How Google shows you ads



This ad may be based on:

- General factors about the placement of the ad, agreed upon by the publisher (ex: website, app) and the advertiser
- Information collected by the publisher. The publisher partners with Google to show ads

Esto parece indicar que la campaña de publicidad en línea de Miguel Uribe Turbay ha hecho más hincapié en la cantidad, a la vez dirigida y no dirigida. Esto es también consistente con el resto de análisis realizados.

¿Y ha habido alguna interacción por medio del correo electrónico?

Sí, y se recibieron en relación a cada una de las ciudadanas:

- 4 correos de parte de la campaña de Claudia López en el buzón de correo de la ciudadana virtual Karolina Lopez[4];
- 5 correos de parte de la campaña de Miguel Uribe Turbay en el buzón de correo de la ciudadana virtual Karolina Uribe[5];
- 1 correo de parte de la campaña de Hollman Morris en el buzón de la ciudadana virtual Karolina Morris[6];
- no se recibieron correos de parte de la campaña de Carlos Fernando Galán.

En el anexo "Primer correo electrónico enviado por los candidatos" se pueden observar el primer correo electrónico de cada una de las campañas, pero podemos destacar que sólo los correos de Claudia López contienen un vínculo o enlace para darse de baja de la lista de correo[7]. Las listas de correo de las campañas de Hollman Morris y Miguel Uribe Turbay no cuentan con esa posibilidad a través de sus *e-mail* y este último utilizó, como ya vimos arriba, el píxel de rastreo, que funcionó como "pixel de apertura"[8], para la instalación de *cookies*.

¿Alguna interacción por redes sociales?

En este caso, los resultados fueron limitados. Nos planteamos dos hipótesis no excluyentes para explicar este resultado:

1. Nuestros perfiles "ficticios" en Facebook y Twitter tienen un comportamiento muy distinto de un perfil real. En particular no cuentan con amigos y seguidores y su número de interacciones es bajo.
2. Los candidatos que analizamos no usaron estas herramientas para publicidad en línea a través de redes sociales.

Apuntamos más a la hipótesis uno y pensamos que existe aún campo para expandir la investigación en esta línea, en relación al uso de publicidad en redes sociales por parte de las campañas electorales. No obstante, se requeriría para ello el uso de perfiles reales o la creación y uso previo de perfiles ficticios que cuenten con un comportamiento similar a un perfil real.

4. Con fechas entre el 25/09 y el 19/10 y con títulos, en orden de recepción: "Ayúdanos a cuidar cada voto, ¡conviértete en testigo electoral!", "¿Quieres ayudarnos?" Sé uno de nuestros testigos electorales", "Nos vemos este sábado en el concierto de Doctor Krápula" y "Te invito mañana a concierto en Plaza imperial".

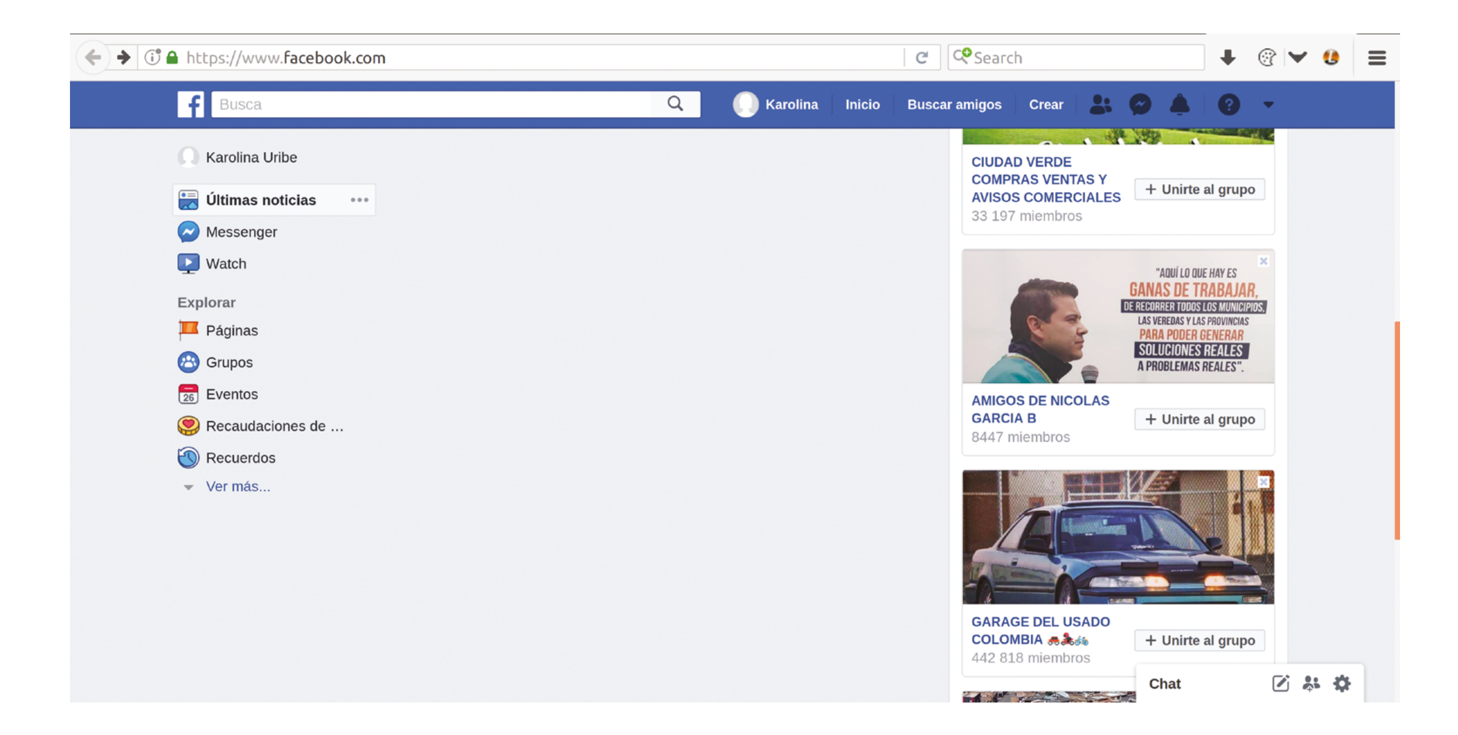
5. Con fechas entre el 22/09 y el 26/09 y con títulos, en orden de recepción: "Bienvenido al equipo de Miguel Uribe", "En nuestras manos, está el futuro de Bogotá", "Esto es lo que propongo", "Los parques no serán lugares de consumo y venta de drogas" y "¿POR QUÉ HAY TANTAS PERSONAS SUMÁNDOSE A ESTE MOVIMIENTO?".

6. Con fecha del 30/09 y con título: "Thank you for registering for our event". Se ha probablemente usado el texto por defecto generado por la solución. Ya que ni el título en inglés y el contenido (ver anexo "Primer correo electrónico enviado por los candidatos") son adaptados al contexto de la elección.

7. "Darse baja de la lista", ver anexo "Primer correo electrónico enviado por los candidatos".

8. Es una práctica común que los correos enviados tengan lo que se llama un pixel de detección de apertura, que informa el servidor de que se abierto y/o leído el correo. La instalación de una *cookie* de rastreo por el servidor en respuesta (caso de Miguel uribe Turbay) no es tan común.

En relación a **Facebook** observamos desde el perfil de Karolina Uribe, vinculado a la campaña de Miguel Uribe Turbay, apareció una proposición de unirse al grupo del candidato que fue electo como Gobernador de Cundinamarca, Nicolás García, aunque no podemos asegurar que ambas interacciones estén vinculadas con el sitio web del candidato a la Alcaldía.



En cuanto a **Twitter**, lo único que se pudo notar son propuestas de tendencias vinculadas con las campañas políticas (*hashtags* o grupos). El orden de presentación de las mismas es distinto en función del perfil utilizado, presentándose en general primero aquellas tendencias más afines a la ciudadana virtual.

Karolina López



Karolina Galán



Karolina Morris



Karolina Uribe



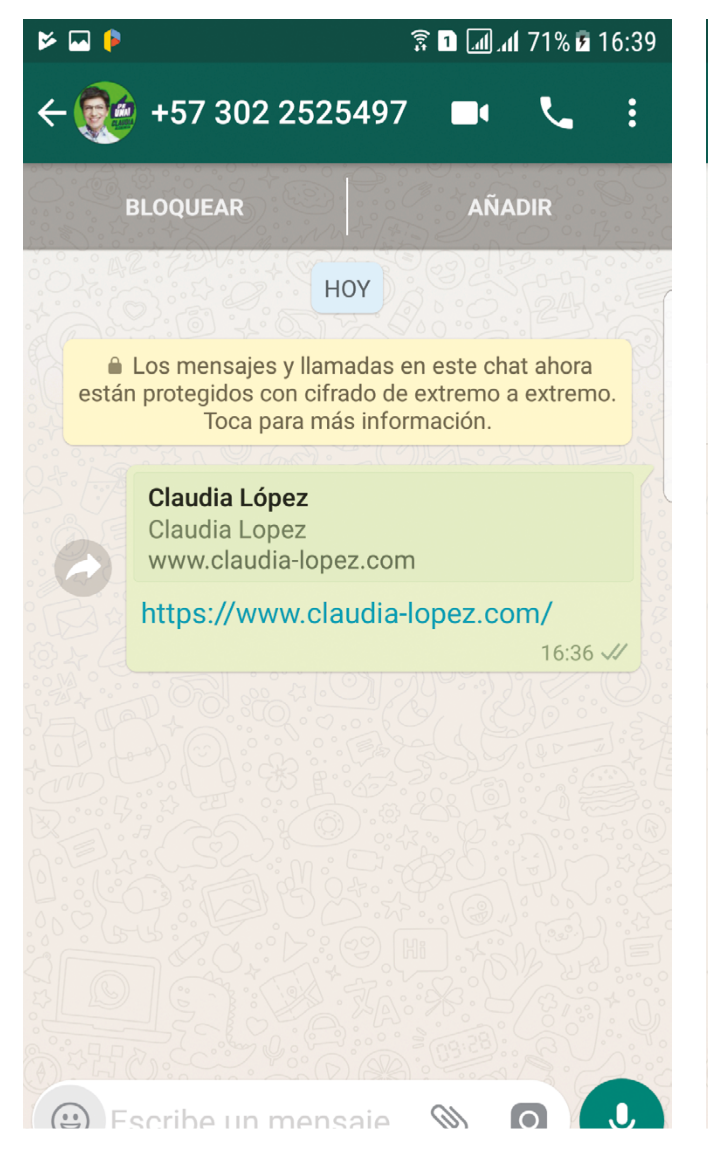
Es posible que lo anterior sea el resultado del algoritmo de Twitter y no de campañas de publicidad dirigida por parte de los candidatos. Lo que muestra es que se acentúa el “fenómeno de burbuja”, proponiendo primero tendencias que supuestamente le van a gustar al usuario.

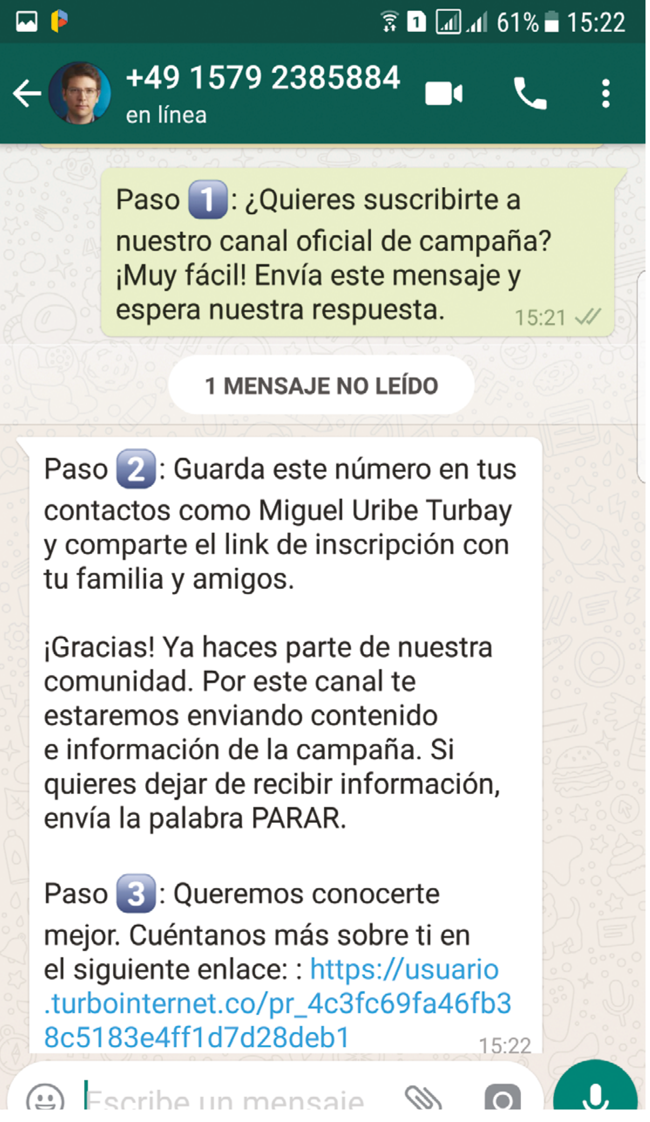
Sin embargo, surge una cuestión interesante: ¿Cómo Twitter obtuvo información sobre nuestras ciudadanas virtuales para que sus algoritmos hicieran esta categorización? Esto implica que probablemente una de las herramientas o empresas involucradas haya compartido con Twitter, y quizá con otros terceros, información de los perfiles. Esta hipótesis es una invitación a seguir investigando.

¿Y qué pasó con los números de teléfono?

Aunque algunos de los formularios web lo incluían entre sus campos, no se recibieron SMS ni llamadas en los números de las ciudadanas virtuales. Sin embargo, Claudia López y Miguel Uribe implementaron en sus sitio web funcionalidades de interconexión con el servicio de WhatsApp a través, respectivamente, de las herramientas: *BeeApp* y *Messenger People*.

En ambos casos se necesitaba que el usuario o usuaria se registraran activamente. El proceso no fue sencillo, ni fluido, por lo que es posible que muy pocos usuarios lo utilizaran. El único efecto del registro fue la recepción de los siguientes mensajes:



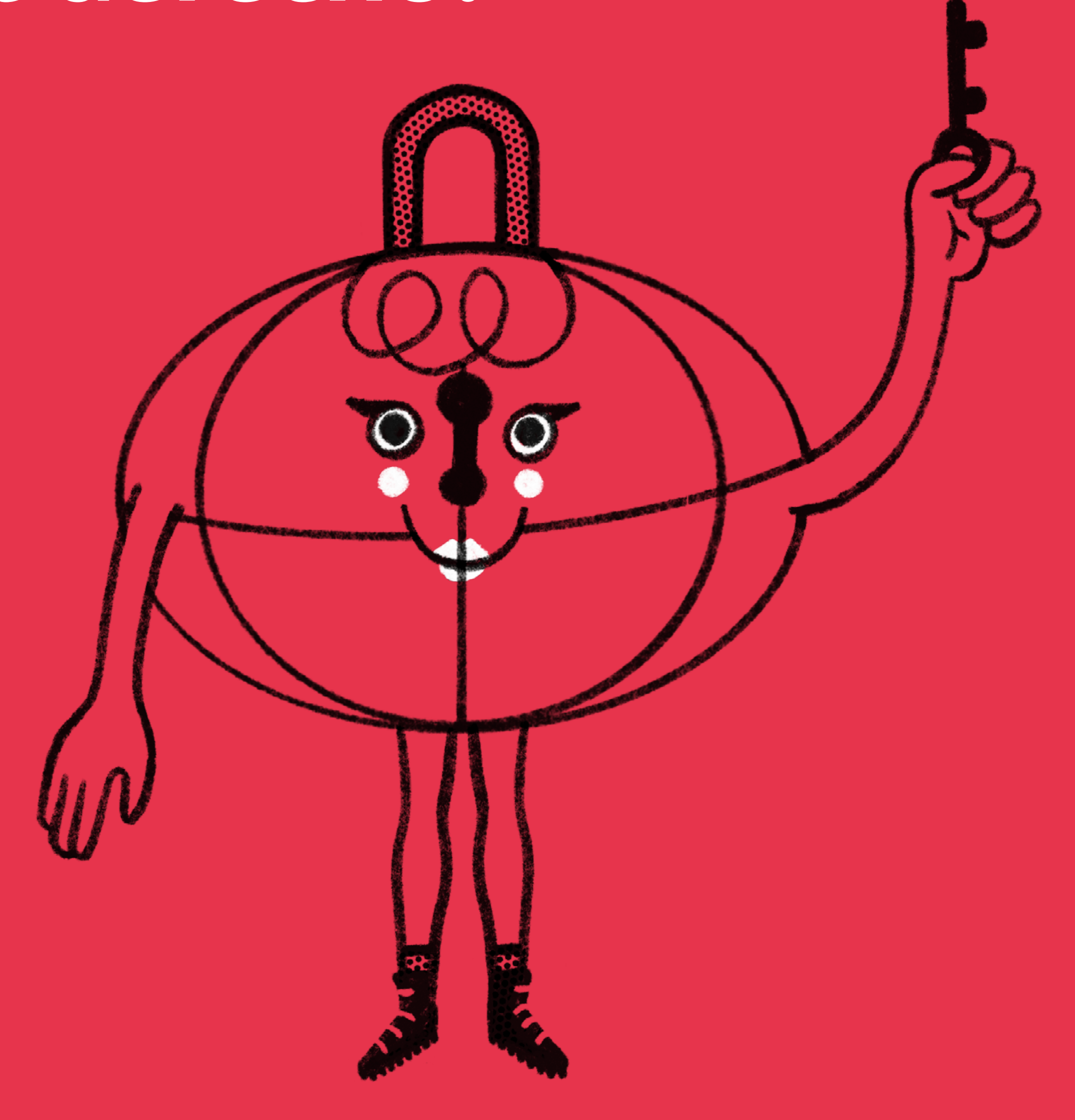


No se recibieron otros mensajes. **Por que pensamos que ambos candidatos estuvieron experimentando nuevas posibilidades con estas herramientas, pero sin usarlas completamente**.

A los efectos de completar el análisis, realizamos el cuestionario “Cuéntanos más sobre ti” (ver anexo “Formulario “Turbo Internet” de Miguel Uribe Turbay”) que aparece en el mensaje de WhatsApp de la campaña de Miguel Uribe Turbay. Este es manejado por la empresa Turbo Internet[9], que vendría a completar la larga lista de empresas terceras que reciben todos parte de nuestros datos en la interacción digital con su campaña. Así, se suma a Amazon, MailChimp (envío de correos), Mautic, Naveg DMP, Google y Messenger People (WhatsApp).

9. http://www.turbointernet.com/

Del técnico al abogado ¿cómo se lee desde el derecho?



Datos y su recolección por formulario

A los efectos de relacionar los resultados de los análisis técnicos con las implicaciones jurídicas, partimos del artículo 15 de la Constitución Política, base de la construcción del régimen de protección de datos en nuestro país:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

Este artículo consagra el habeas data como derecho fundamental, conceptualizado por la Corte Constitucional en la sentencia T-729 de 2002[1]:

> El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales.

¿Y qué son los datos y qué tipos hay para el derecho? Los datos son unidades de información, representaciones simbólica (con números, letras, gráficos, etc.) que permiten compartir o transmitir información.

1. Corte Constitucional, Sentencia T-729 de 2002. M.P. Eduardo Montealegre

JAMES RODRÍGUEZ	Esto es un dato. En este caso, una sucesión de letras
(Nombre y apellido)	Este es el tipo de información que contiene, un nombre y apellido

Al derecho le importa el tipo de información que contienen los datos y los posibles impactos que dicha información puede tener en los derechos de las personas. Por ejemplo, conocer mi opinión política puede llevar a discriminación en algunos contextos. Por ello, las categorías más importantes de datos para nuestro ordenamiento, y cuya regulación es distinta, son las siguientes:

Dato personal: contiene información que se puede vincular con persona determinada o determinable.

Dato sensible: contiene información que afecta a la intimidad y puede generar su discriminación, como la opinión política, las convicciones religiosas, los datos de salud o el origen étnico.

Dato público: este concepto es más complejo porque no supone una definición clara como los anteriores. En general, es público el dato que como tal es calificado por la Constitución o la Ley y que no es sensible[2]. A nuestros efectos, son ejemplos de datos públicos el nombre, estado civil u oficio, toda vez que son recogidos en documentos públicos como la cédula.

Con estas definiciones, los formularios de los candidatos recogían datos públicos y datos personales:

2. La ley 1266 de 2008, que recoge el concepto de dato público, señala que es aquel que no sean privados o semiprivados. Estas dos últimas categorías no se recogen en la ley 1581 ni el decreto 1377, normatividad de referencia para este capítulo. Por ello, hemos escogido en la definición el uso del término "dato sensible".

Tipo de dato	Claudia L.	Hollman M.	Carlos F. G.	Miguel U.
Público	Nombre	Nombre	Nombre	Nombre
Público	Apellido	Apellido	Apellido	
Personal	Teléfono	Teléfono	Teléfono	Teléfono
Personal	*E-mail*	*E-mail*	*E-mail*	*E-mail*
Personal	Localidad	Localidad	Localidad y puesto	
Personal		Organización		
Público			Cédula	
Personal			Intereses temáticos	
Personal			Intereses localidad	

La importancia de conocer el tipo de dato ante el que nos encontramos radica en en los derechos que, como titulares de los mismos, tenemos así como en las obligaciones que los terceros deben cumplir para recolectar, almacenar, usar, circular o suprimir[3] estos datos.

3. Estas acciones se enmarcan en lo que se denomina "tratamiento de datos".

Como titulares, tenemos derecho a[4]:

- Conocer, actualizar y rectificar los datos personales frente a estos terceros.
- Revocar el consentimiento para el tratamiento y solicitar la supresión de nuestros datos ante un tratamiento que no respete el ordenamiento.
- Ser informado por parte de los terceros del tratamiento que se le da a nuestros datos.
- Acceder gratuitamente a los datos que hayan sido objeto del tratamiento.
- En los casos en que es necesario el consentimiento para el tratamiento, solicitar prueba del mismo.
- Presentar quejas ante la Superintendencia de Industria y Comercio, que es la autoridad colombiana de datos frente al tratamiento por parte de privados[5].
- No estar en la obligación de consentir al tratamiento de datos para acceder a un bien o servicio, especialmente si se trata de la captura o recolección de datos sensibles[6].

En coherencia con esto, los terceros que traten nuestros datos tienen una serie de obligaciones, entre las que destacamos aquellas relacionadas con la obtención del consentimiento para el tratamiento y la información sobre el mismo.

El **consentimiento**[7] debe ser previo e informado, y en medio que pueda ser consultado posteriormente. La excepción legal por la cual puede darse lugar

4. Art. 8 de la ley 1581 de 2012

5. Frente al tratamiento por parte de entes públicos, es la Procuraduría General de la Nación la autoridad de datos.

6. Art. 6, Decreto 1377 de 2013 “por el cual se reglamenta la Ley 1581 de 2012”

7. Art. 9 de la ley 1581 de 2012

al tratamiento de datos personales sin contar con el consentimiento previo de la persona se relaciona, en concreto[8]:

- A la captura y procesamiento de datos públicos.
- A la captura y procesamiento de datos relacionados con el Registro Civil de las Personas.
- A la captura y procesamiento de datos para atender una urgencia médica o sanitaria.
- Los datos que son requeridos por una entidad pública o administrativa en desarrollo de sus funciones legales o por orden judicial.
- Tratamiento de datos con fines históricos, estadísticos o científicos.

Con independencia de que no sea necesario el consentimiento, los terceros tienen **obligaciones de información** sobre el tratamiento cuya ausencia puede suponer, no solo el incumplimiento de la norma, sino un obstáculo para el ejercicio por parte del titular de sus derechos. La información debe incluir[9]:

- El tratamiento que se le dará a los datos.
- La finalidad de dicho tratamiento.
- Los derechos con los que cuenta el titular de los datos y el procedimiento para su ejercicio.
- La identificación, dirección física, electrónica y teléfono del responsable del tratamiento.
- La naturaleza no obligatoria de aquellas respuestas relacionadas con datos sensibles o datos de niñas, niños o adolescentes.
- El período de vigencia de la política y de las bases de datos.

Regresando al caso de los candidatos a la Alcaldía de Bogotá, los sitios web de las candidaturas de **Hollman Morris** y **Miguel Uribe Turbay** no cuentan con información alguna respecto a la política de tratamiento de datos, a

8. Art. 10 de la ley 1581 de 2012

9. Art. 12 de la ley 1581 de 2012 y art. 13 del decreto 1377 de 2013

pesar de que en las mismas se recolectan datos personales. Como decíamos, la ausencia de información no solo es problemática por sí misma, también porque supone la imposibilidad de ejercer los derechos por parte del titular de la información al desconocerse la identidad del responsable de los datos y el canal para el ejercicio de los mismos.

Distinto es el caso de los sitios web de las candidaturas de **Claudia López** y **Carlos Fernando Galán**. Ambas cuentan con información respecto al tratamiento de datos[10] (denominadas política de datos y declaración de privacidad respectivamente) que responden, además, a modelos estandarizados y extendidos en su uso en las páginas web en nuestro país. En cuanto a los requisitos normativos mínimos de las políticas de tratamiento, la siguiente tabla muestra el cumplimiento:

10. El decreto 1377 de 2013, que reglamenta la ley 1581 de 2012, establece una diferencia entre "políticas de tratamiento", cuyo contenido mínimo se recoge en el artículo 13, y "aviso de privacidad", estableciendo el artículo 15 su contenido mínimo. Por su parte, el artículo 14 señala que se utiliza el aviso de privacidad de modo subsidiario y en los casos en los que no sea posible poner a disposición del Titular las políticas de tratamiento de la información. Este es el caso de avisos de privacidad en edificios, a través de carteles, pero es difícil de imaginar en un escenario digital, en una página web, en el que no hay restricciones de texto.

Artículo 13, decreto 1377 de 2013	Claudia López[11]	Carlos F. Galán[12]
Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable	Sí. La candidata aparece como responsable con sus datos identificados en la sección "Disposiciones Generales"	Parcial. Además de no contar con el teléfono del responsable, este sería la campaña como persona jurídica, pero se facilita una cédula de ciudadanía en lugar de un NIT.
Tratamiento al cual serán sometidos los datos y finalidad del mismo	Parcial. Si bien la sección "Fines de recolección de datos" es clara en cuanto a estos, no están tan claramente expresadas las acciones de tratamiento.	Sí. Se encuentran separadas, estando la finalidad en la sección homónima, mientras el tratamiento se encuentra separado en "políticas generales de tratamiento" y "política especial de tratamiento de fotos".
Derechos del titular	Sí. Sección "Derechos de los Titulares de Datos Personales"	Sí. Sección "Derechos de los Titulares"
Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización	Sí. En la sección homónima, que incluye también el procedimiento para el ejercicio de los derechos.	Sí. La política detalla cuál será la organización interna en la campaña en relación a las responsabilidades con el tratamiento de datos en la sección "organización interna". Incluso se detallan las funciones del llamado "oficial de bases de datos" en la sección homónima. De igual manera, se detallan los deberes de los encargados del tratamiento, en caso de existir.
Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización	Sí. Ver cuadro superior.	Sí. En la sección "gestión de consultas, reclamos, solicitud de actualizaciones".
Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos	No. No se especifica la fecha de entrada y ha de deducirse que la vigencia de la misma está vinculada al desarrollo de la campaña.	No. A pesar de que existen hasta dos secciones relacionadas con la vigencia, esta refiere "a los datos personales" y no a la política de tratamiento en sí.

11. En el caso de Claudia López, la información todavía es visible en la web https://www.claudia-lopez.com/pages/politica-de-datos. Curiosamente, la candidatura a optado por situar en dicha página tanto la política de tratamiento como el aviso de privacidad, ubicada justo después de la anterior.

12. La web de la candidatura ya no se encuentra online.

Consecuencias de los defectos en la información

Un ejemplo real, resolución 54559 de 2014 de la sic[13]

En 2014, un candidato al Senado de Cambio Radical fue denunciado por hacer recolección de datos personales para una base de datos con finalidad electoral. Esta se realizaba a través de un formulario en papel en el que solicitaba nombre y apellidos, cédula, estado civil, profesión u oficio, nombre del cónyuge, número de hijos, dirección, municipio y teléfono. Si bien no se recogía a través de una web, el funcionamiento es el mismo: solicitud de datos a través de un formulario.

Esta situación fue denunciada ante la SIC, señalando los denunciantes que no se cumplía la obligación de informar sobre el tratamiento y finalidad del mismo. En más, en este caso, además, se inducía a error pues, en el mismo documento, se incluía publicidad sobre el programa de Vivienda Gratuita en el departamento de Córdoba y el formulario se antecedía de "Queremos ser beneficiarios de Vivienda Gratis", programa del Ministerio de Vivienda que nada tenía que ver con la recolección de los datos.

El denunciado, para su descargo, argumentó que:

- Los datos eran públicos, no siendo necesario obtener consentimiento.
- Que no siendo necesario obtener consentimiento, tampoco lo era informar sobre el uso y finalidad de los datos.
- Que a pesar de la información del programa del Ministerio de Vivienda, era evidente que la recolección se hacía en sede de una campaña política por aparecer información de la afiliación política del candidato, así como sus datos de contacto.

13. Disponible íntegra en https://www.sic.gov.co/sites/default/files/files/Res%20No_%2054559%20de%202016.pdf

En su resolución, la Superintendencia de Industria y Comercio apunta a que:

- Los datos que se recogieron no eran todos públicos. Aquellos más allá del nombre, cédula, profesión y estado civil son datos personales.
- Con ese cambio en la calificación de los datos, el consentimiento era necesario.
- Y dicho consentimiento había de ser previo, expreso e informado.
- Siendo esto último imposible por la ausencia de cualquier información sobre el tratamiento y finalidad del mismo.

Lo que supuso una sanción económica para el denunciado.

¿Cuál es el estatus jurídico de las *cookies* en colombia?

Como vimos arriba, las *cookies* son informaciones que se inscriben a distancia en nuestros computadores para facilitarnos, en principio, la navegación web. En particular porque cuando ingresamos a un sitio web, enviamos al servidor las *cookies* para fines técnicos o para conocer nuestros hábitos y preferencias de navegación y ofrecernos la versión de la web que más se adaptaría a aquellos. Este rastreo web permite, por ejemplo, que nuestras redes sociales queden abiertas una vez hemos ingresado, de manera que no tengamos que escribir el usuario y contraseña con cada clic.

Sin embargo, supone también que, a través de nuestra navegación web, la información de las *cookies* sea compilada por terceros. Esto nos remite a la regulación de protección de datos que hemos estado viendo puesto que la información recogida por la lectura de *cookies* puede referir a una persona identificada o identificable, toda vez que se recogen desde nuestros dispositivos. Es decir, si la información obtenida por la lectura de las *cookies* se compila por un tercero en una base de datos para su tratamiento, se aplica con normalidad la ley 1581 de 2012. En este sentido se pronunció la Superintendencia de Industria y Comercio en un concepto emitido el 9 de agosto de 2016[14].

14. Número de radicado 16-172268. Disponible en: https://www.sic.gov.co/recursos_user/boletin-juridico-sep2016/conceptos/datos_personales/16172268-proteccion-datos-9-ago-2016.pdf

En cuanto a lo analizado por nuestros candidatos, observamos que solo dos de los cuatro candidatos utilizaron una banda de *cookies* para informar sobre las mismas. No obstante, también vimos que, en ambos casos, la totalidad de las *cookies* eran instaladas antes de cualquier aceptación por parte del usuario, estableciéndose una especie de presunción de aceptación total y en bloque de las mismas.

Banda *cookies* en el sitio de Claudia López

Este sitio web utiliza cookies para garantizar que obtenga la mejor experiencia en nuestro sitio web. Leer más Aceptar

Banda *cookies* en el sitio de Miguel Uribe Turbay

Utilizamos cookies para asegurarnos de brindarle la mejor experiencia en nuestro sitio web. Si continúa utilizando este sitio, asumiremos que está de acuerdo con esto.
LO ENTIENDO

En el caso del candidato **Miguel Uribe Turbay**, la información de la banda de *cookies* se limitaba a señalar "[u]tilizamos cookies para asegurarnos de brindarle la mejor experiencia en nuestro sitio web. Si continúa utilizando este sitio, asumiremos que está de acuerdo con esto", sin mayor información en otro enlace. Estas dos líneas se alejan de los estándares de información que estamos viendo y que consagra la ley 1581 de 2012.

La banda de *cookies* de la candidata **Claudia López** incluye un "leer más". Sin embargo, como señalamos arriba, el enlace redirige a www.cookiesandyou.com, una web con información genérica sobre qué son las *cookies* y cómo controlarlas y deshabilitarlas. En este sentido, y al igual que en el caso anterior, la información ofrecida en la banda y a raíz de la misma no se alinea con los estándares establecidos en la normatividad colombiana.

Finalmente, aunque no lo hace a través de una banda de *cookies*, la candidatura de **Carlos Fernando Galán** incluye información al respecto en una sección específica de su política de privacidad. En este sentido, la candidatura

trata la información de las *cookies* en la misma lógica que el resto de datos e incluye, en la sección respectiva:

- Una explicación somera de qué son las *cookies* y su funcionalidad.
- El tratamiento y finalidad que se le da a la información obtenida de las *cookies*.
- La posibilidad del titular de borrar en cualquier momento las *cookies*, como modo de ejercitar los derechos del titular.
- La aplicación del resto de la política también a las *cookies*.
- Que las *cookies* a las que se refieren son las de origen, no haciéndose responsables por las *cookies* de terceros. En este sentido, recordemos que la web del candidato es de las que tienen menor presencia de *cookies* de terceros, habiendo visto incluso que la presencia de las de *marketing* (del servicio *doubleclick*) venían instaladas por causa de usar el servicio de YouTube.

Tratamiento de datos sensibles por las candidaturas a la alcaldía

Hablamos antes de los datos sensibles y su importancia por la potencialidad de derivarse, de su uso, impactos a derechos fundamentales más allá de la privacidad, como la discriminación. En relación a estos, la norma prohíbe su tratamiento con unas excepciones[15]:

- Los titulares hayan dado consentimiento explícito a dicho tratamiento. Es decir, un consentimiento concreto, no siendo válido un consentimiento general o en bloque.
- Sea necesario el tratamiento para salvaguardar un interés vital del titular.
- El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos

15. Art. 6 de la ley 1581 de 2012

regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

- Sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un juicio.

- El tratamiento sea con fines históricos, estadísticos o científicos. En este caso, debe suprimirse la identidad de los titulares.

Es decir, los datos sensibles requieren obligaciones reforzadas en relación al consentimiento y la información. En este sentido, recordamos que los datos referentes a opiniones políticas son de naturaleza sensible, por lo que lo serán también algunos de los datos recogidos en sede de campaña política. Más cuando se refiere a la simpatía con la misma.

Sin embargo, no existen menciones a datos sensibles en las políticas de tratamiento de los candidatos **Carlos F. Galán** y **Claudia López** que vimos arriba. Esta última recoge las definiciones de datos privados y semiprivados, pero no tienen incidencia en el resto del clausulado.

Podría pensarse que aplicaría, en principio, la excepción al tratamiento de datos sensibles por tratarse de "organismos sin ánimo de lucro con finalidad política", sin embargo, una interpretación restrictiva de esa excepción extiende su aplicación tratándose de los datos de afiliados, miembros o militantes[16] de la organización sin ánimo de lucro con finalidad política, siendo cuestionable que la entrega de datos sensibles por una persona interesada en una campaña como la de elecciones a la Alcaldía, suponga de manera alguna la adquisición de dicha categoría. No obstante, aunque se entendiese de alguna forma que la excepción en cuestión resulta aplicable, todavía sería necesaria una autorización explícita por el titular del dato para permitir el suministro de sus datos sensibles a terceros, lo cual demandaría una autorización independiente a la genérica que encontramos en las políticas de tratamiento de datos de ambos candidatos.

16. No en vano, la Corte Constitucional señaló en su sentencia C-748 de 2011 que la Sala encuentra que la excepción del literal c) se encuentra justificada en tanto (i) se refiere a datos que circulan solamente al interior de las organizaciones enunciadas; y (ii) es propio de tales organizaciones recoger y procesar datos sensibles de sus miembros o personas que mantienen contacto con ellas, precisamente porque la razón de su existencia está ligado con alguno de los ámbitos personales que da lugar a datos sensibles.

Recapitulando...

Hemos intentado transmitir de modo fácilmente comprensible los principios básicos sobre el funcionamiento de internet y las herramientas de rastreo de navegación y los hemos puesto a prueba en relación al funcionamiento de las campañas electorales. Para contextualizar estos conceptos nos centramos en la experiencia de la ciudadanía que surge como fruto del uso de estas herramientas por las campañas, así como la normativa relacionada, particularmente desde la perspectiva de protección de datos y privacidad.

Esperamos que esta lectura haya despertado su curiosidad por estos temas y contribuido a incrementar sus capacidades en la materia. Algunas de las pruebas que hemos hecho se han compartido con el objetivo de que puedan ser fácilmente utilizadas y que los resultados se puedan comenzar a comprender.

Sin embargo, también esperamos que las campañas electorales tengan en consideración algunas de las cuestiones aquí señaladas, sobre todo desde una perspectiva jurídica, pues el estudio de caso de las campañas para la Alcaldía de Bogotá despierta varios cuestionamientos.

...Concluyendo...

No es posible tener una imagen completa de qué ha ocurrido con los datos de nuestras ciudadanas virtuales, a pesar de las pruebas técnicas, de acudir a los mecanismos de transparencia activa y leer en detalle las políticas de tratamiento de datos y otros documentos similares.

A esta imposibilidad contribuyen tanto el cumplimiento defectuoso de la norma que señalamos en el capítulo anterior como una práctica centrada en la mera forma. Es decir, los mecanismos de transparencia cumplen superficialmente con la norma y no atienden realmente su razón de ser. Un ejemplo de este hecho ocurre con la información publicada a través de la herramienta Cuentas Claras[1] (ver anexo "Transparencia de la publicidad digital: Cuentas Claras"). A pesar de la finalidad de transparencia de este portal, no fue posible conocer a través de la información consignada por las campañas todos los terceros que intervienen en el tratamiento de nuestros datos. En particular, no encontramos aquellos que habíamos detectado a través de las pruebas técnicas.

Esto nos invita a considerar dos reflexiones preliminares:

- El cumplimiento de la normativa como mera formalidad es una obligación que debe ser repensada. Esta es una labor de los responsables que han de conocer la norma y el por qué de la misma, pero también del resto del ecosistema que debe plantearse si la debilidad que permite un cumplimiento vacuo radica en la norma en sí o en el desarrollo, la interpretación, la vigilancia, sanción o en varios de estos puntos.

- En relación con lo anterior, el cumplimiento se ha de hacer pensando en la ciudadanía como titular de derechos. Y esto supone hacerlo de modo comprensible para las personas y desplegando mecanismos de ejercicio de derechos razonables. Las pruebas técnicas, el conocimiento jurídico y el trabajo realizado en esta investigación supera con creces lo que se puede exigir a las personas para el conocimiento de lo que ocurre con su información y el ejercicio de sus derechos.

1. Cuentas Claras (https://www.cnecuentasclaras.gov.co) es el aplicativo web por medio del cual las campañas electorales tienen obligatoriamente que reportar sus ingresos y gastos. A través de la misma web, la ciudadanía puede consultar dicha información.

... Y recomendando

Sobre la base de estas conclusiones y del estudio de caso que hemos ido presentando, podemos ofrecer una serie de aprendizajes y cuestionamientos que serán útiles tanto en retrospectiva, para las candidaturas del año pasado, como para la consideración por parte de futuras candidatas y candidatos. Las presentamos por medio de esta tabla sintética de hallazgos y recomendaciones:

Sobre Información y protección de datos

	Claudia López	C.F. Galán	Hollman Morris	Miguel Uribe
Hallazgos	Sí, pero incompleta + banda de *cookies* inefectiva	Sí	No	No + banda de *cookies* inefectiva

Recomendaciones:

- Implementar una política de tratamiento de datos personales completa, que incluya explícitamente el uso que se hace de los datos sensibles, en particular con las finalidades vinculadas con el *marketing* digital.
- Incluir mayor información respecto de las técnicas de publicidad usadas y los terceros a los que se transmiten datos personales para ello.
- Implementar mecanismos para dar de baja a los inscritos consistente con el medio de inscripción.

Sobre el Alojamiento de datos (sitio web)

	Claudia López	C.F. Galán	Hollman Morris	Miguel Uribe
Hallazgos	Estados Unidos / California y Canadá (Shopify e In Motion)	Estados Unidos / Washington (Amazon)	Estados Unidos / Arizona (Go Daddy)	Estados Unidos / Washington (Amazon)

Recomendaciones:

- Evaluar los impactos respecto a la privacidad, en relación al cumplimiento de la ley de habeas data, de la elección de las empresas que traten y alojen los datos personales que se recojan, y la ubicación de las mismas.

- Evaluar la dispersión posible de estos datos frente a la multiplicación de las herramientas utilizadas: sitio web, envíos de correos, empresas de *marketing*, servicios de interconexión de mensajería, etc. En particular, el caso de la campaña Miguel Uribe es destacable en este sentido.

Sobre la utilización de diferentes técnicas de rastreo

	Claudia López	C.F. Galán	Hollman Morris	Miguel Uribe
Rastreo con *cookies* accidental	Sí. *Cookies* publicitarios de Google (doubleclick) por el uso de YouTube			Uso directo del servicio publicitario de Google
Rastreo por *cookies* debido al uso de servicios de *Marketing*	Sí. Shopify: campañas de publicidad de tipo *retargeting*	No	No	Sí. Uso directo de tres tipos de herramientas: Google, Mautic, Navegg DMP
Rastreo con técnicas "furtivas"	No detectado	No detectado	No detectado	Sí. Uso de técnicas de *fingerprinting* (herramienta Beta de Mautic)
Interconexión de las técnicas de rastreo	No detectado	No detectado	No detectado	Sí, interconexión con los correos que instalan *cookies*. Interconexión posible con Facebook

Recomendaciones:

- Evaluar el impacto del uso de herramientas (vídeo, analytics, etc) que puedan generar rastreo en conexión con datos personales, eventualmente sensibles.

- Evaluar el impacto y de la legalidad del uso de herramientas de *marketing* digital, en conexión con la naturaleza de la información, vinculada a una campaña política, y la expresión del consentimiento de la persona usuaria.

- Evaluar el impacto y la legalidad del uso de herramientas que generen un rastreo furtivo y permiten sobrepasar las medidas de protección de la privacidad implementadas por las personas (ej: *fingerprinting*).

En general, pensamos que los esfuerzos de las campañas han de ir dirigidos a adecuar sus prácticas de uso de tecnologías digitales en campaña al espíritu de las normas de protección de datos y privacidad, trascendiendo la práctica del mero cumplimiento formal. Subyace un cambio de paradigma, una superación del cumplimiento celoso en las formas por el temor a las consecuencias y una apropiación de la transparencia y respeto de derechos como base para las relaciones con la ciudadanía. Resulta, quizá como última elucubración, curioso que en procesos tan basados en la confianza como las campañas electorales, una mirada un poco profunda al uso de tecnologías digitales no se encuentre con espacios de confianza sino con dificultades en términos de transparencia. No es solo que falte información sino que no hay mecanismos claros y efectivos para que las personas que participan de estos espacios puedan ejercer sus derechos a la información y a la privacidad. Volviendo a nuestro querido Hanlon, sea esta última línea no un reproche, sino una invitación.



Fundación Karisma

<K+LAB>

INDELA